
Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
 Volume 24, Issues 3, pp. 257–276, DOI 10.12694/scpe.v24i3.2381

PROTECTING DATA AND PRIVACY: CLOUD-BASED SOLUTIONS FOR INTELLIGENT TRANSPORTATION APPLICATIONS

SURJIT SINGHA *AND RANJIT SINGHA†

Abstract. The interaction between transportation networks and intelligent transportation systems has been revolutionized by cloud computing. However, the reliance on cloud-based solutions raises security and privacy concerns. This article examines the challenges of safeguarding data and privacy in intelligent transportation applications and emphasizes the potential of cloud-based solutions to resolve these issues. Organizations can protect sensitive data and user privacy by employing encryption, access controls, threat detection mechanisms, and privacy protection measures. Adopting these cloud-based solutions will encourage the extensive adoption of intelligent transportation applications while infusing users and stakeholders with confidence.

Key words: Data security, Privacy protection, Intelligent transportation applications, Cloud-based solutions, Confidentiality, Integrity, Access control.

1. Introduction. Intelligent transportation systems have transformed our mobility and interaction with transportation networks. By utilizing sophisticated technologies such as cloud computation, these systems provide numerous benefits, including improved traffic management, increased safety, and enhanced efficiency [11]. However, the growing reliance on cloud-based solutions raises security and privacy concerns. This article will discuss the challenges of safeguarding data and privacy in intelligent transportation applications and how cloud-based solutions can address these issues [23].

Intelligent transportation systems have revolutionized how we move and interact with transportation networks. By leveraging advanced technologies such as cloud computing, these systems offer numerous benefits, including improved traffic management, enhanced safety, and increased efficiency [35]. However, the increasing reliance on cloud-based solutions also raises concerns about data security and privacy.

As intelligent transportation applications generate vast amounts of data, ranging from real-time traffic information to personal user details, safeguarding this data is crucial to prevent unauthorized access, data breaches, and potential misuse [6]. Cloud-based solutions provide a robust framework to protect sensitive information by employing various security measures [21].

This article will explore the challenges of protecting data and privacy in intelligent transportation applications and discuss how cloud-based solutions can address these concerns. We will delve into the importance of data security, including encryption and access control mechanisms, secure data storage and backup options, and threat detection and intrusion prevention measures. Additionally, we will examine the significance of privacy protection, including anonymization and pseudonymization techniques, privacy by design principles, and data governance and compliance frameworks. By implementing these cloud-based solutions, organizations can mitigate risks, enhance user trust, and foster the widespread adoption of intelligent transportation applications. It is imperative to balance the advantages of cloud computing and the need for robust data security and privacy protection.

This article explores the significance of data security and privacy in intelligent transportation applications, investigates how cloud-based solutions can effectively address these concerns, and highlights the role of encryption, access controls, threat detection, privacy-by-design principles, and data governance frameworks in ensuring a secure and privacy-aware environment. The article focuses on applying various data security and privacy measures in the context of intelligent transportation systems, mainly through cloud-based solutions. While the provided abstract and content outline provides a comprehensive overview of the topic, they lack

*Kristu Jayanti College (Autonomous), Bengaluru, India (surjitsingha@gmail.com)
†Christ University, Bengaluru, India (ranjitsingha@gmail.com)

specific mathematical or analytical components. However, it's possible to incorporate mathematical concepts or analyses in certain areas. The article mentions robust encryption techniques like Advanced Encryption Standards (AES). A potential mathematical analysis could involve explaining the mathematical basis of AES encryption, including the substitution-permutation network (SPN) structure and the mathematical operations (such as substitution and permutation) involved in the encryption process. The article briefly discusses real-time threat detection using machine learning algorithms. A mathematical analysis could delve into the types of machine learning algorithms used, such as anomaly detection algorithms (like Isolation Forest) and their mathematical foundations, including the formulation of anomaly scores and decision boundaries. The article mentions Role-Based Access Control (RBAC) and multi-factor authentication. A mathematical analysis might involve explaining the mathematical principles behind RBAC, such as role hierarchies, permissions matrices, and the mathematical representation of access control policies. The article introduces privacy-enhancing techniques like data anonymization and pseudonymization. A mathematical analysis could explain the concepts of k-anonymity, l-diversity, and differential privacy, showcasing the mathematical mechanisms to protect individual privacy while retaining data utility. The article discusses integrating privacy into system design. A mathematical analysis could include formal methods for specifying and verifying privacy properties in system architectures, ensuring that privacy guarantees are mathematically upheld throughout the system's lifecycle. The article mentions data governance frameworks. A mathematical analysis could involve discussing data classification methods, retention policies, and the mathematical modelling of data lifecycle management processes.

2. Statement of Problem. Intelligent transport applications play a crucial role in current transport systems, generating and processing immense quantities of sensitive data. Nevertheless, ensuring the security and confidentiality of this data presents significant challenges. Unauthorized access, data breaches, and potential misconduct can have severe repercussions, eroding user confidence and system integrity. To resolve these issues, it is necessary to investigate how cloud-based solutions can provide a secure framework for protecting sensitive data in intelligent transportation applications.

This article examines the significance of data security in intelligent transportation applications and the mechanisms and solutions provided by cloud platforms to ensure confidentiality, integrity, controlled access, and regulatory conformance. This article endeavours to contribute to developing strategies and best practices for implementing secure and privacy-enhancing cloud-based solutions in intelligent transportation applications by delving into the topics mentioned above. The article will specifically address the following research questions:

- Given the nature of the data involved and the potential threats, what is the significance of data security in intelligent transportation applications?
- How can cloud-based solutions address intelligent transportation applications' data security and privacy concerns?
- In the context of intelligent transportation applications, what mechanisms and solutions do cloud platforms provide to assure confidentiality, integrity, controlled access, and regulatory compliance?

This article examines the challenges and opportunities associated with data security and privacy in intelligent transportation applications by reviewing these research questions. The findings will contribute to advancing this field's knowledge and provide industry professionals, policymakers, and researchers with practical guidance for instituting effective security measures—privacy-enhancing practices in cloud-based intelligent transportation systems.

3. Research Objectives. To demonstrate how cloud-based solutions provide a robust framework for safeguarding sensitive data, assuring confidentiality, integrity, controlled access, and regulatory compliance in intelligent transportation applications. To demonstrate the importance of data security and privacy protection in cloud-based intelligent transportation applications and to emphasize the solutions and mechanisms offered by cloud platforms to address these issues effectively.

4. Research Methodology. A systematic literature review methodology will investigate the importance of data security in intelligent transportation applications and the role of cloud-based solutions in addressing data security and privacy concerns. This research method involves a systematic and rigorous approach to identifying, selecting, and analysing relevant scholarly articles, research papers, and publications in the field.

Identification of Research Objective and Research Questions. The problem statement's research objective and questions have been directed to the literature review. Examining the mechanisms and solutions cloud platforms offer to guarantee confidentiality, integrity, and regulated access.

Search Strategy. To identify pertinent literature, a thorough search strategy is developed. Multiple electronic databases, including ACM Digital Library, IEEE Xplore, ScienceDirect, and Google Scholar, will be searched using keywords and search terms pertinent to data security, privacy, cloud computing, and intelligent transportation application research. Additional sources, such as conference proceedings, journals, and relevant reports, will also be considered. The following are the search terms used:

- Data security, intelligent transportation applications, privacy protection, and cloud-based solutions.
- Integrity or confidentiality or access control; regulatory compliance and cloud computing.
- Data storage and backup and cloud-based solutions.
- Threat detection or intrusion prevention.
- Anonymity or pseudonymization and privacy by design.
- Frameworks for data governance and compliance, sophisticated transportation applications.
- User confidence or privacy safeguards and cloud-based solutions.

Inclusion and Exclusion Criteria. Inclusion and exclusion criteria were formulated to ensure the selection of pertinent studies. These criteria include the publication date within the last two decades, the topic-related research focus, the methodologies utilized, and the applicability of the findings to the research questions addressed. The selection procedure is conducted in an organized and open manner.

Study Selection. The identified studies were subjected to a two-step selection process based on the inclusion and exclusion criteria defined. The relevance of titles and abstracts to the research questions is determined initially through a preliminary screening. The full-text articles of potentially relevant studies were evaluated for ultimate inclusion in the literature review.

Data Extraction and Analysis. Data extraction required systematically collecting pertinent information from the chosen studies, such as research objectives, methodologies, critical findings, and limitations. The extracted data were organized and synthesized to identify common themes, trends, and patterns associated with data security in intelligent transportation applications and the role of cloud-based solutions.

Critical Appraisal. To ensure the findings' validity and dependability, the chosen studies' quality and importance were critically evaluated. This evaluation assessed the research design, methodology, data analysis techniques, and authors' credibility.

5. Synthesis and Interpretation. The data synthesized from the selected studies were analyzed, summarized, and interpreted to address the research questions. The findings were presented coherently and logically, highlighting the key insights, gaps, and suggestions. The results were reviewed regarding the study's goals and questions. Research gaps are highlighted, and the literature's limitations are discussed. Finally, the findings and implications of the systematic literature evaluation regarding the value of data security and the function of cloud-based solutions for intelligent transportation applications are summarized. This research provides a comprehensive overview of the existing literature on data security in intelligent transportation applications and the effectiveness of cloud-based solutions in addressing data security and privacy concerns by employing a systematic literature review methodology. The systematic approach assures the review procedure's rigour, transparency, and reproducibility, contributing to the credibility and validity of the research results.

6. The Importance of Data Security. Intelligent transport solutions provide substantial quantities of data, including real-time traffic information as well as user-specific data [18]. It is essential to ensure the safeguarding of this data against unauthorised access, breaches, and possible abuse. Cloud-based solutions provide a comprehensive framework for protecting sensitive data via the implementation of diverse security mechanisms.

Data security is of utmost importance in intelligent transportation systems, since it plays a critical role in safeguarding sensitive data [8]. According to [20], these apps produce substantial quantities of data, including real-time traffic updates, vehicle tracking data, user-specific information, and financial transactions. In order to

uphold the confidence of users and stakeholders and mitigate the risks of unauthorised access, data breaches, and possible exploitation, it is essential to prioritise the preservation of confidentiality, integrity, and accessibility of this data [13].

Cloud-based solutions provide a rigorous foundation for data protection, which becomes advantageous for intelligent transport applications. Within this particular setting, many elements serve to underscore the significance of data security.

This research underscores the need to ensure the availability and ease of access to data. The evaluation of access control policies is supported by various mathematical foundations. These include formal languages that are utilised to specify policies, algorithms that enforce these policies, system models that verify their compliance with security-related properties, Bayesian probability and statistical analysis, homomorphic encryption techniques that enable computations on encrypted data, Z-score or Mahalanobis distance for measuring statistical significance, partially ordered sets and lattice structures for organising access control relationships, and the mathematical principles underlying encryption algorithms such as Rivest–Shamir–Adleman or Advanced Encryption Standard.

The method is sometimes referred to as Rivest–Shamir–Adleman, after the surnames of its creators. The aforementioned cryptographic technique is extensively used in asymmetric encryption for the purpose of ensuring the safe transmission of data and the generation of digital signatures. The RSA encryption algorithm relies on the mathematical features inherent in big prime numbers and the inherent challenge of factoring them. The technique produces a pair of cryptographic keys, consisting of a public key and a private key. The public key is used for the purpose of encryption, while the private key is utilised for decryption.

The Advanced Encryption Standard (AES) is a widely used symmetric encryption technique that has emerged as the prevailing standard for securing data via encryption. The Advanced Encryption Standard (AES) is a cryptographic algorithm that acts on blocks of data. It provides support for key lengths of 128, 192, or 256 bits. The technique uses a range of mathematical processes to provide strong data encryption, including substitution-permutation networks (substitutions and permutations) and critical expansion.

The RSA and AES algorithms are well-recognised cryptographic techniques that play a crucial role in safeguarding data confidentiality and security across a range of applications, such as communication, data storage, and digital signatures.

6.1. Confidentiality. Intelligent transport systems often manage very sensitive data, including user identities, payment details, and location information. The encryption technologies used in cloud computing effectively obfuscate the data, making it incomprehensible to those who lack proper authorization. The study conducted by [14]. Encryption ensures that data remains safe and unavailable to unauthorised parties, even in the event of interception, unless the appropriate decryption keys are used. Cloud-based solutions have many benefits in intelligent transportation systems, including enhanced scalability, real-time data processing capabilities, and cost-effectiveness. Nevertheless, the growing dependence on cloud services presents a significant obstacle in safeguarding sensitive data and maintaining confidentiality. The incorporation of cloud-based technologies in intelligent transportation necessitates the implementation of strong safeguards to ensure the protection of privacy and security for both users and the transportation infrastructure. In the subsequent discussion, we will examine the significance of maintaining confidentiality in cloud-based intelligent transportation systems and investigate essential approaches for safeguarding sensitive data. Transportation apps that are considered innovative often have the need to regularly gather and retain personal information that is of a sensitive nature. This information may include GPS coordinates, details pertaining to vehicle identification, and user preferences. Ensuring confidentiality is of utmost importance in order to mitigate unauthorised access and improper use of this data, hence safeguarding the privacy rights of persons.

According to [36], cloud-based solutions play a crucial role in the administration and control of traffic. Preserving the confidentiality of traffic data, specifically pertaining to real-time vehicle flow and congestion information, is of utmost importance in order to mitigate any malevolent actions that may impede the transportation network or compromise public safety. Collaboration between transport authorities and research institutes may be facilitated via the implementation of novel projects inside cloud platforms. The use of confidentiality measures is necessary in order to mitigate the risk of unauthorised dissemination of intellectual property, proprietary algorithms, and experimental data. The use of effective encryption algorithms for data

at rest and in transit serves to guarantee the data's unreadability in the case of unauthorised access. The encryption protocols TLS and AES are extensively used in many applications. By implementing robust access control measures and using multi-factor authentication, the organisation may ensure that only those with proper authorization are granted access to sensitive data and essential system components. The implementation of role-based access control (RBAC) is a method that limits user access by considering their designated tasks and obligations [17]. This approach mitigates the risk of unauthorised individuals gaining access to sensitive data. APIs play a crucial role in the integration of various components within intelligent transportation applications. The use of authentication and access restrictions in securing APIs serves the purpose of mitigating unauthorised access to confidential backend data.

The implementation of a data minimization plan involves the collection and retention of just the necessary data for specific purposes. The act of limiting the exposure of sensitive information and reducing the possible consequences of a data breach is a recommended practice. The implementation of continuous monitoring and frequent audits of cloud systems facilitates the timely detection of potential vulnerabilities and unauthorised activities. Real-time alerts may be configured to identify and flag any atypical conduct. The implementation of robust data deletion measures serves to mitigate the risks associated with data leakage and illegal access to outdated information. The preservation of confidentiality is of paramount significance due to the sensitive nature of the data used in cloud-based intelligent transportation systems, encompassing personal information, traffic management particulars, and private research data. Transportation authorities and cloud service providers can establish user confidence, cultivate public trust, and effectively implement intelligent transportation systems without compromising data privacy and security by implementing a comprehensive approach to safeguard confidentiality. This approach encompasses various measures such as data encryption, robust access controls, and routine monitoring.

The use of mathematical models holds considerable importance in elucidating the underlying principles of encryption algorithms. These models aid in comprehending many mathematical concepts, including modular arithmetic and exponentiation employed in RSA encryption, as well as the substitution and permutation operations involved in AES encryption. This academic discussion pertains to the mathematical principles behind the production of cryptographic keys. It encompasses several themes such as prime number generation, modular inverse computation, and the mathematical foundation of crucial pairings in the context of asymmetric encryption. The encryption mechanism known as Transport Layer Security (TLS) is generally acknowledged in academic literature as being extensively used. The mathematical foundations of Transport Layer Security (TLS) protocols include fundamental principles such as asymmetric key exchange, including the Diffie-Hellman algorithm, as well as symmetric encryption techniques to ensure the safe transfer of data. The mathematical principles behind Role-Based Access Control (RBAC) include the formal depiction of roles, permissions, and user assignments via the use of set theory or graph theory. Various statistical techniques may be used for the purpose of anomaly identification. These strategies include the establishment of thresholds using measures like as mean and standard deviation, as well as more sophisticated approaches like clustering and outlier detection. This study focuses on the development of mathematical models that aim to quantify the sensitivity of data and determine the least amount of data necessary for specific tasks. These models take into account several elements, such as entropy and information theory, in order to accurately assess the level of sensitivity and the amount of data needed. The use of time series or pattern recognition techniques in mathematical analysis includes the utilisation of statistical approaches to analyse logs and identify trends that might potentially signify security breaches. Cryptographic methods used for ensuring safe data deletion include the utilisation of algorithms such as the Advanced Encryption Standard (AES) in a designated mode, such as AES-CTR, to facilitate the process of data wiping.

6.2. Integrity. The preservation of data integrity is essential to ensuring that data stays unaltered and free from corruption over its entire lifespan. Cloud systems use checksums and digital signatures as mechanisms to safeguard the integrity of data during its storage or transfer processes [22]. The utilisation of mathematical models holds considerable importance in determining the characteristics of secure hash functions, including collision resistance and preimage resistance. These properties guarantee that the task of discovering two distinct inputs that yield identical hash values or reconstructing the initial input from its hash, is computationally impractical. The cryptographic hash functions include mathematical characteristics, namely the avalanche

effect and the challenge of discovering collisions, which guarantee that even little changes in the input data provide hash values that are substantially distinct. The mathematical principles behind MAC algorithms, such as HMAC (Hash-based Message Authentication Code), include the integration of hash functions and secret keys in order to guarantee the integrity of data and mitigate the risk of unauthorised modifications. The mathematical underpinnings of Public fundamental Infrastructure (PKI) include several fundamental components, such as digital certificates, public-private key pairs, and the mathematical algorithms used in the generation and authentication of digital signatures. The mathematical concepts that form the foundation of the security of cryptographic methods. For example, one may elucidate the challenges associated with the factorization of large semiprime integers in the context of the RSA encryption scheme, as well as the discrete logarithm issue as it pertains to specific cryptographic protocols such as Diffie-Hellman. Mathematical analysis offers the potential to investigate many strategies, such as Merkle Trees, that use hash functions to effectively check the consistency and integrity of extensive data structures. The use of mathematical techniques for the identification and rectification of faults in sent data plays a crucial role in preserving the integrity of data in the presence of transmission defects. The birthday paradox is a mathematical notion that has implications for cryptography techniques. This paradox serves as an illustration of the likelihood of two distinct inputs yielding the same hash result, hence emphasising the need for robust cryptographic hash algorithms to ensure data integrity. The inclusion of mathematical principles and analytical approaches might facilitate a more profound comprehension of the methods by which integrity is preserved in cloud-based systems, using several cryptographic methodologies and data verification processes.

6.3. Access Control. The management of data access has significant importance in the context of intelligent transportation systems. Cloud-based solutions enable organisations to effectively deploy strong access control techniques, including multi-factor authentication and role-based access restrictions. The use of these techniques serves to provide stringent controls over data access and modification, hence mitigating the potential for unauthorised individuals to gain in or manipulate the data [25]. A comprehensive examination of the subject matter may include elucidating the mathematical underpinnings of set theory, which serves as the fundamental framework for Role-Based Access Control (RBAC). The ideas of sets, subsets, intersections, and unions are foundational principles in set theory that correspond to the allocation of user roles and permissions. The use of graph theory may be essential in the development of access control systems. A potential avenue for mathematical investigation is the examination of access control via the use of graph theory. In this context, vertices would symbolise users, resources, and permissions, while edges would denote the connections and associations between them. Access control often entails the process of making determinations predicated upon specific criteria. Boolean algebra, a mathematical discipline concerned with binary variables and logical processes, is pertinent in this context. Boolean expressions have the potential to elucidate access control rules and situations via the use of mathematical analysis. Access control techniques often include discrete decision-making and logical activities. The use of discrete mathematics principles, such as permutations and combinations, enables the representation of various access situations and facilitates the examination of potential combinations of permissions and roles.

Formal methods include a set of mathematically rigorous approaches that are used to describe, verify, and validate software and systems. A mathematical analysis may be used to examine the utilisation of formal techniques in order to quantitatively demonstrate the satisfaction of specified security features by access control rules, hence assuring their accurate implementation. The article discusses the concept of multi-factor authentication. A mathematical examination may explore the mathematical principles behind cryptographic methods used in multi-factor authentication (MFA), including the utilisation of cryptographic hash functions to create one-time passwords and the mathematical characteristics associated with public-private key pairs. The process of access control often includes the development and administration of cryptographic keys. The security of several cryptographic methods used in access control relies on fundamental notions in number theory, including prime numbers, modular arithmetic, and the discrete logarithm issue. The assessment of access control strategies may include the use of probabilistic models. A mathematical analysis may be used to examine the application of probability theory in evaluating the probability of certain access situations or assessing the possible consequences of policy alterations. Including these mathematical ideas and analyses may contribute to a more holistic understanding of the technological underpinnings of access control methods in cloud-based

intelligent transportation systems. .

6.4. Threat Detection and Intrusion Prevention. Cloud systems use advanced security methods to identify and mitigate possible security risks. In the realm of cloud infrastructure, the continuous monitoring of network traffic and activity is facilitated by intrusion detection systems, firewalls, and anomaly detection algorithms. According to [28], the occurrence of any potentially suspicious behaviour triggers an alarm, prompting the implementation of appropriate countermeasures in order to mitigate the risk of unauthorised access and data breaches. The article discusses the use of anomaly detection methods. A mathematical study may include an exploration of statistical concepts such as the mean, standard deviation, and Gaussian distributions, which are often used to characterise typical patterns of activity. Alerts for suspicious behaviour may be triggered by deviations from these patterns. The process of intrusion detection often incorporates machine learning methodologies. Machine learning methods, such as decision trees, support vector machines, and neural networks, may be elucidated via mathematical analysis. These algorithms are designed to discern patterns that signify infiltration, hence enhancing the security of systems. The process of detecting anomalies often involves the analysis of time series data. A mathematical examination may be conducted to investigate signal processing methodologies for the purpose of preprocessing and analysing time-dependent data, including but not limited to Fourier transforms and wavelet analysis. Bayesian networks can effectively represent intricate interconnections between variables. A mathematical examination may be conducted to explore the mathematical aspects of Bayesian networks, which serve as a means to express interdependencies among various events and facilitate probabilistic intrusion detection. The use of information theory principles, such as entropy and mutual information, enables the quantification of the level of randomness or predictability inherent in data. A mathematical study has the potential to explore the use of these notions in detecting deviations from anticipated patterns in network traffic or system behaviour. The article discusses the monitoring of traffic inside cloud infrastructure. The field of graph theory is capable of representing and analysing various network architectures. A mathematical examination might be conducted to investigate the use of graph theory principles, such as nodes, edges, and connectedness, in the field of network analysis. This study would aim to uncover atypical patterns or nodes exhibiting aberrant behaviour. The article discusses the implementation of alert systems that are triggered by the detection of potentially suspicious activities. Bayesian inference is a statistical method that entails the revision of probability in light of new data. A mathematical study may be conducted to explore the use of Bayesian inference in updating the probability of an event being classified as an incursion, as further data is acquired. An inquiry might be conducted to examine the use of queueing theory in the context of intrusion prevention. Queueing models are valuable tools for the prediction and analysis of system behaviour under varying traffic loads. They may assist in the identification of atypical patterns that may signify an intrusion attempt. The identification of potential risks often entails the discernment of recurring behavioural patterns. A mathematical analysis may include the exploration of pattern recognition methodologies, such as clustering algorithms or hidden Markov models, which are used to detect repetitive patterns within datasets. The use of mathematical ideas and analysis may provide valuable insights into the technological components of threat detection and intrusion prevention systems within cloud-based intelligent transportation applications.

6.5. Data Storage and Backup. Intelligent transportation applications benefit from cloud-based solutions' scalable and dependable data storage options. Data can be stored on redundant and geographically dispersed servers, which reduces the risk of data loss caused by hardware malfunctions or natural disasters. Regular data backups enhance data resiliency and facilitate rapid recovery during unanticipated events [16]. The article discusses the concept of redundant servers. A mathematical analysis has the potential to investigate several ideas derived from probability and statistics in order to evaluate the probability of failure for specific components as well as the whole system. The quantification of concepts such as mean time between failures (MTBF) and mean time to repair (MTTR) allows for the mathematical design of systems that possess desirable degrees of fault tolerance. The article discusses the use of servers that are geographically scattered.

A mathematical study may include the exploration of principles derived from graph theory or geometry in order to optimise the distribution of data among servers, hence achieving efficient data access, minimising latency, and enhancing fault tolerance. The implementation of redundancy in storage often incorporates strategies such as erasure coding. The mathematics behind Reed-Solomon codes, which are used in data storage systems for error detection and repair, may be elucidated by a rigorous mathematical analysis. This analysis

serves to guarantee the integrity of data, even in the event of server failures. The article discusses the need to implement frequent data backups. Probability theory may be examined via a mathematical study within the framework of data loss and backup techniques. This may include the computation of the chance of data loss as time progresses, as well as the identification of the most advantageous backup frequency and redundancy measures. Queueing theory may be used to analyse the optimal utilisation of resources, including bandwidth and storage capacity. A mathematical study may be used to investigate the utilisation of queueing models in the allocation of resources for data storage and retrieval. This analysis takes into account many elements such as data access patterns and system loads. Although not expressly stated in the text, it is worth noting that data deduplication is a widely used approach in the field of data storage. A mathematical study may be conducted to explore the mathematical concepts behind data deduplication techniques, which aim to detect and remove redundant data in order to enhance storage efficiency.

Data compression is often used in order to achieve efficient storage. A mathematical study may delve into the underlying principles of data compression methods, such as Huffman or arithmetic coding, by examining information theory topics like entropy and coding theory. Mathematical models are used for the evaluation of the dependability and accessibility of storage systems. For instance, the use of Markov models or Petri nets enables the modelling of storage components' behaviour and the anticipation of system dependability across various circumstances. The article discusses the phenomenon of rapid recuperation in the face of unforeseen circumstances. An investigation in mathematics may be conducted to examine the correlation between the frequency of backups, recovery time goals (RTO), and the possible loss of data (recovery point objective - RPO), therefore offering valuable insights for the development of efficient backup systems. The use of mathematical ideas and analyses may enhance comprehension of the technological concerns involved in guaranteeing dependable and robust data storage and backup procedures inside cloud-based intelligent transportation systems.

6.6. Compliance with Regulations. Numerous nations have stringent data security and privacy regulations, such as the European Union's General Data Protection Regulation (GDPR). Cloud platforms provide organizations with frameworks and instruments for maintaining regulatory conformance. These tools assist in defining data retention policies, consent management mechanisms, and audit trails for data access, ensuring compliance with applicable regulations [15]. In intelligent transportation applications, data security is of the utmost importance. Cloud-based solutions provide a robust framework for safeguarding sensitive data, ensuring its confidentiality, integrity, and controlled access. Organizations can mitigate risks and preserve users' and stakeholders' confidence in intelligent transportation systems by instituting encryption, access controls, threat detection mechanisms, and robust storage and backup solutions [12]. Mathematical models have the potential to be formulated in order to guarantee adherence to legislation, such as the General Data Protection Regulation (GDPR). These models may include the establishment of mathematical principles and criteria that govern data processing operations in order to ensure compliance with legal obligations. Privacy impact assessments include the evaluation of possible privacy hazards that may arise from the processing of data. Mathematical analysis may be used to estimate privacy concerns by using probability and effect evaluations. This approach aids organisations in making well-informed choices about their data handling practices. The article discusses the implementation of audit trails as a means of monitoring and documenting data access activities. A mathematical study may be used to investigate graph theory principles in order to construct a model for data provenance, which facilitates the tracing and documentation of data lineage and historical information, hence enabling traceability and accountability. Temporal logic is a valuable tool for the expression and verification of material features, including but not limited to data retention regulations and permission expiry. A mathematical study may be conducted to examine the use of temporal logic in formalising and verifying compliance rules across a period of time. Consent management encompasses the practice of monitoring and recording user consent pertaining to the processing of their data. A mathematical study may be used to investigate the utilisation of graph theory in representing the interconnections among users, data processing activities, and permission status, with the aim of facilitating effective consent management. Formal verification procedures include the use of mathematical methodologies to rigorously ascertain the adherence of systems to defined attributes. A mathematical study may be used to examine how conventional practices might effectively exhibit adherence to regulatory mandates, therefore guaranteeing that data processing operations conform to legal benchmarks. The essay discusses the importance of reducing risks and maintaining trust. Probability theory may be used in

a mathematical study to examine risk assessment, specifically in the calculation of the probability of security breaches or non-compliance incidents. This analysis can provide valuable insights for developing effective risk management methods. Privacy metrics may be measured in order to evaluate the level of privacy safeguarding in the context of data processing. A mathematical examination may explore the computation and use of privacy metrics, such as k-anonymity or differential privacy parameters, in order to guarantee adherence to privacy standards. Organisations often encounter the need for data sharing while maintaining compliance with regulations. The use of game theory principles presents a viable approach for the modelling of interactions among entities engaged in data sharing. This entails a comprehensive analysis of the incentives and legal limitations that influence the behaviour of these parties. The essay discusses the importance of adhering to regulatory standards. The use of Bayesian inference allows for the continual monitoring and updating of compliance evaluations, taking into account fresh evidence and adjusting to changes in data processing operations and regulatory requirements. The inclusion of these mathematical principles and analyses may provide a more holistic understanding of the technological and legal dimensions involved in guaranteeing regulatory adherence and safeguarding data integrity within cloud-based intelligent transportation systems.

7. Encryption and Access Control. Encryption, which entails encapsulating data to make it opaque to unauthorized users, is crucial to data security. Cloud platforms provide robust encryption mechanisms to safeguard data during transmission and storage [1]. Furthermore, the implementation of access control techniques, such as multi-factor authentication and role-based access restrictions, may effectively limit access to those who have been granted authorization. The mathematical underpinnings of cryptography include several principles, including encryption algorithms, cryptographic keys, and the intricacies of the encryption and decryption procedures. This includes mathematical techniques, such as modular arithmetic, which are used in encryption methods. The article discusses the implementation of strong encryption techniques. The administration of cryptographic keys plays a significant role in the field of encryption. A mathematical analysis may be used to investigate topics like key generation, key exchange protocols (e.g., Diffie-Hellman), and the mathematical principles that guarantee the security of cryptographic keys. The notion of Public Key Infrastructure (PKI) encompasses mathematical principles associated with asymmetric cryptography, including the mathematical correlation between public and private keys, as well as the computational intricacy of certain mathematical problems that form the foundation of PKI's security measures. The discussion might revolve around several notions in information theory, including entropy and the notion of complete secrecy, as first proposed by Claude Shannon. These principles elucidate the theoretical boundaries of safe communication and the inherent indeterminacy that encryption cannot fully eradicate. The field of number theory plays a crucial role in the development and implementation of the RSA encryption algorithm. The study of encryption may include an examination of the mathematical aspects pertaining to RSA encryption, including the mathematical characteristics of prime numbers, modular exponentiation, and the challenges associated with the factorization of large semiprime integers. Elliptic Curve Cryptography (ECC) is a cryptographic method that falls under asymmetric encryption. An examination of the algebraic structures of elliptic curves and their applications in cryptographic operations may be undertaken via mathematical study. Although not expressly stated, steganography is a technique that entails concealing the existence of information by embedding it into other data. The importance of information theory and statistical analysis in constructing efficient steganographic methods may be investigated via a mathematical study. Access control techniques often include logical processes. The field of Boolean algebra, which pertains to the manipulation of binary variables and logical processes, is applicable in this context. A mathematical analysis may be used to elucidate the manner in which Boolean expressions can establish access control rules and criteria. Graph theory may be used to depict access control schemes. A mathematical study may be conducted to examine the use of graph theory principles, such as nodes and edges, in the modelling of access connections and permissions. The use of finite automata theory extends to the modelling of access control policies and the establishment of the underlying logic for implementing certain licences and limitations. Formal methods include a set of mathematically rigorous approaches used for the purpose of system verification. A mathematical analysis may be used to examine the applicability of conventional approaches in validating the accuracy of access control rules and procedures. The inclusion of mathematical ideas and research may contribute to a more profound comprehension of the technological foundations of encryption, access control, and data security procedures inside cloud-based intelligent transportation systems.

7.1. Secure Data Storage and Backup. Cloud-based solutions provide intelligent transportation applications with reliable and scalable data storage alternatives. According to [31], storing data on redundant and geographically distributed servers may mitigate the potential risks of data loss resulting from hardware breakdowns or natural catastrophes. The use of regular data backups serves to improve the resilience of data and expedite the process of recovery in unforeseen circumstances. Mathematical models can be constructed to evaluate the dependability and accessibility of data storage systems. Dependability engineering principles, such as failure rates, may be employed to quantitatively assess the trustworthiness of individual servers and the overall system architecture. The use of queueing theory is relevant in the modelling of storage systems since it enables the analysis of many performance metrics, such as waiting times for data access, system utilisation, and reaction times under varied workloads. The article discusses the potential for data loss from hardware problems or natural calamities. Probability theory enables the evaluation of the probability of these occurrences transpiring and the computation of their possible consequences on data availability. The topic of regular data backups is being addressed. Mathematical analysis encompasses the computation of recovery time goals (RTO) and recovery point objectives (RPO) by leveraging backup frequency, hence facilitating the optimisation of backup techniques. Erasure coding encompasses the use of data redundancy methodologies. A mathematical study may be conducted to explore the mathematical principles behind erasure coding techniques, which generate duplicate data pieces to facilitate data recovery in the event of partial data loss. The presence of geographically scattered servers suggests the use of data replication. Graph theory may be employed to represent and analyse data replication schemes, guaranteeing the optimal dissemination of data copies over several servers to minimise latency. Bayesian networks have the capability to effectively define and analyse interdependencies and potential hazards within the context of disaster recovery planning. A mathematical study may investigate the use of Bayesian networks in evaluating the probable consequences of different catastrophe scenarios. Data deduplication is a storage optimisation technique that entails identifying and eliminating redundant data. Using information theory principles, such as entropy, allows for quantifying data redundancy and optimising deduplication algorithms. The article discusses the use of servers that are distributed across different geographical locations. Geometric principles, such as distance metrics, may be used to optimise the positioning of servers to achieve data redundancy and mitigate the impact of geographical disturbances. Graph colouring methods distribute data to servers so duplicate copies are kept on distinct servers, reducing the likelihood of simultaneous loss. Markov models enable the examination of server behaviour by assessing the possibilities of failure and recovery. This analytical approach facilitates predicting system performance and behaviour over a certain period. Using mathematical ideas and analyses may provide valuable insights into the technological issues involved in developing dependable and robust data storage and disaster recovery methods within cloud-based intelligent transportation systems.

7.2. Threat Detection and Intrusion Prevention. Cloud platforms utilize advanced security measures to detect and mitigate potential hazards. Intrusion detection systems, firewalls, and anomaly detection algorithms constantly monitor cloud infrastructure traffic and activity [27]. Any potentially illicit behaviour triggers an alarm system, prompting the implementation of appropriate countermeasures to thwart unauthorised entry and safeguard against the compromise of sensitive information. The topic of anomaly detection techniques is discussed. Statistical principles, such as the calculation of mean, variance, and standard deviation, may be used to establish benchmarks for typical behavioural patterns and detect departures from these patterns, which may indicate possible risks. Machine learning methodologies, such as clustering algorithms or support vector machines, may be effectively used to identify discernible patterns of behaviour that indicate the presence of intrusion. The mathematical principles underlying the training and use of machine learning models are pertinent in this context. Probability theory, specifically Bayesian inference, may be used to evaluate the likelihood of certain acts being malevolent by integrating past information with newly acquired evidence. Information theory concepts, such as entropy, can quantitatively measure the level of randomness or unpredictability in data. Anomalies often have elevated entropy levels, a characteristic that may be recognised by mathematical means. The topic of discussion pertains to the surveillance of network traffic inside cloud infrastructure. The field of graph theory is used to represent and analyse network topologies. This framework examines many elements, such as nodes, edges, and connectedness, to uncover atypical patterns or nodes exhibiting aberrant behaviour. The anomaly identification process often entails examining and analysing time series data. Time

series analysis is a statistical technique encompassing many methods, such as autoregressive integrated moving average (ARIMA) models and exponential smoothing. These methods detect and analyse trends, patterns, and anomalies within organised chronological data. Bayesian networks can effectively represent and capture the interdependencies between various occurrences. A mathematical study may be conducted to investigate the capacity of Bayesian networks to represent the interconnections among different system activities and their potential as indicators of threats. The identification of concealed data, such as malicious software, may be addressed via steganalysis methodologies. The process entails using mathematical analytic techniques to identify hidden patterns or variations within data, which serve as indicators for potential risks. The field of queueing theory enables the analysis of traffic patterns to detect abnormalities. Mathematical techniques may identify anomalies by comparing observed queue lengths and waiting times with their corresponding predicted values. Mathematical optimisation approaches may be used to establish rules for detecting risks. The regulations mentioned above possess the capability to develop thresholds for identifying suspicious activity by using mathematical analysis of past data. The article discusses the concept of intrusion prevention. Graph colouring algorithms can analyse access control links and detect probable patterns of unauthorised access. Including these mathematical principles and analyses may facilitate a more profound comprehension of the technological underpinnings of threat detection and intrusion prevention techniques in cloud-based intelligent transportation systems.

7.3. Privacy Protection. Data security and user privacy protection are of utmost importance in intelligent transport systems. Cloud-based solutions provide a wide range of methods aimed at safeguarding privacy. Differential privacy is a mathematical paradigm that quantifies the extent to which an individual's privacy is compromised when their data is included in a dataset. The use of differential privacy principles may effectively safeguard the privacy of a dataset by minimising the impact of every data point on the overall privacy of the information. The privacy models discussed below pertain to the alteration of data so that it becomes indiscernible within a collective of persons. Mathematical evaluations may be used to investigate the efficacy of various models in maintaining privacy while enabling data usefulness. Using concepts derived from information theory, such as entropy, allows quantifying the degree of information or privacy that is compromised throughout the data exchange process. The examination of information loss may assist in achieving a harmonious equilibrium between data usefulness and the protection of privacy. Mathematical methodologies, such as safe multi-party computing and homomorphic encryption, can facilitate data mining on encrypted data while guaranteeing the preservation of confidentiality for sensitive information throughout the analysis process. Zero-knowledge proofs and rapid multiparty computing are cryptographic protocols designed to maintain data confidentiality by allowing it to be utilised for specific purposes without disclosing the actual contents. The mathematical underpinnings of these methods may be investigated. The Laplace mechanism is used to introduce random perturbations into query replies, safeguarding the anonymity of individual users. The mathematical studies may be directed towards determining the ideal quantity of noise to be added, while simultaneously ensuring the preservation of data usefulness. The introduction of controlled noise derived from entropy may be used to disturb data and provide privacy protection. Mathematical analysis may be used to investigate the optimal level of entropy that can be introduced to strike a balance between preserving privacy and enabling meaningful analysis. These methods include modifying data to eliminate personally identifying information. Mathematical computations may evaluate the efficacy of anonymization techniques in mitigating the potential for re-identification. Secure multi-party computation protocols refer to a computational framework whereby numerous parties collaborate to perform a function while ensuring the confidentiality of their respective inputs. The mathematical principles behind these protocols may be examined to understand their potential use in privacy-preserving analytics. The safeguarding of privacy requires a comprehensive comprehension of the movement of data. Graph theory ideas may be used to represent and analyse data flows, hence enabling the identification of possible privacy risks and the proposal of strategies to strengthen security. Methods such as -differential privacy include monitoring and allocating a privacy budget. Mathematical studies may be used to investigate the optimal allocation of funding to ensure both effectiveness and the preservation of a satisfactory degree of privacy. By integrating mathematical principles and conducting empirical investigations, one may get valuable insights into the technological underpinnings of privacy protection measures used in cloud-based intelligent transportation systems.

7.4. Anonymisation and Pseudonymisation. Prior to being stored or processed in cloud-based systems, personal data has the potential to undergo anonymization or pseudonymization techniques to safeguard the identities of users. This methodology entails the replacement of personally identifiable information with distinct identifiers or the deliberate obscuring of the data, so impeding the ability to establish a direct connection between the data and particular people. Entropy from information theory, specifically the Entropy and De-identification framework, may be used to evaluate the extent of information loss that occurs through anonymization or pseudonymization. Mathematical analysis may facilitate the identification of an appropriate equilibrium between the value of data and the protection of privacy. The privacy models of K-anonymity and L-diversity aim to guarantee the indistinguishability of data inside a given group. Mathematical analysis may be used to investigate the influence of these models on the quality of data and the preservation of privacy. Probability theory enables the evaluation of the potential for re-identification by analysing the retained information in anonymized or pseudonymized datasets. Mathematical analysis can calculate the probability of a successful re-identification assault. Through mathematical principles about utility, it becomes possible to examine the extent of information loss that occurs during the process of anonymization or pseudonymization, as well as to assess if the resulting data retains an adequate level of value for analytical purposes. Using graph theory ideas enables the analysis of linkages between anonymized data and possible external data sources, hence facilitating the evaluation of data linkage and re-identification risk. Hash functions can be used for pseudonymizing data. Mathematical analysis enables examining the characteristics of cryptographic hash functions and their implications for safeguarding data integrity and mitigating re-identification vulnerabilities. Mathematical computations may be used to examine the inherent trade-offs between the value of data and the safeguarding of privacy, so aiding in the determination of the optimal degree of anonymization or pseudonymization that simultaneously maximises both goals. Latent Variable Models include the task of identifying latent variables that account for the observable data.

Mathematical analysis may be used to investigate the potential of latent variable models in facilitating pseudonymization processes while maintaining the integrity of data attributes. The use of mutual information, a concept from information theory, allows for quantifying the extent to which pseudonymization reduces the leaking of information. Mathematical methods may be used to quantify the extent to which pseudonymization effectively mitigates information leakage. Statistical Disclosure Control encompasses many techniques aimed at safeguarding against re-identification assaults. Mathematical computations may be used to investigate the impact of noise injection, aggregation, and suppression on the likelihood of re-identification. Mathematical optimisation methods may be used to identify the optimal pseudonymization approach that maximises data value while ensuring robust privacy protection. The integration of mathematical ideas and studies may provide valuable insights into the technological underpinnings of anonymization and pseudonymization processes in intelligent transportation systems hosted on cloud platforms.

7.5. Privacy by Design. Incorporating privacy concerns into the design and development of intelligent transportation applications is essential. Cloud-based solutions can enforce privacy by design principles, ensuring privacy safeguards are built into application development [34]. This strategy helps reduce privacy risks and assures compliance with privacy laws. Privacy by Design (PbD) is a proactive and ethical approach that prioritises data protection and privacy throughout the entire lifecycle of intelligent transportation cloud applications [34, 26]. PbD emphasises incorporating privacy concerns into the design, architecture, and development of systems instead of addressing privacy concerns as a supplement [4]. Privacy by Design plays a crucial role in ensuring the confidentiality, integrity, and ethical use of sensitive data in intelligent transportation applications that leverage cloud-based solutions [7]. Privacy by Design stipulates that cloud-based conveyance systems should be designed with data protection and privacy [3]. By being proactive, it is possible to identify and mitigate potential privacy risks and vulnerabilities before they become significant problems. Privacy by Design (PbD) encourages privacy-friendly defaults, assuring that the maximum level of privacy protection is implemented by default to user data. Users should not be required to configure their privacy settings to protect their data.

Privacy by Design emphasises that data protection measures should not hinder cloud-based transit applications. Instead, Privacy by Design (PbD) enhancing technologies [5], Privacy by Design (PbD) incorporated seamlessly to facilitate optimal user experiences [37].

Privacy by Design (PbD) considers data security throughout the entire data lifecycle, including data acquisition, storage, processing, and disposal. It safeguards data at every stage, minimising the possibility of unauthorised access.

The transparency and comprehensibility of privacy rules for intelligent transportation apps are crucial in enabling users to make informed choices about the sharing and utilisation of their data. The recommended approach is to selectively gather and retain just the necessary data for the specific objective, thereby reducing the likelihood of disclosing confidential information. In order to safeguard the identities of individuals while maintaining the research and analytical value of the data, it is recommended to use methods such as anonymization or pseudonymization. To ensure the security of data, it is essential to use encryption techniques throughout both transmission and storage processes. It is also crucial to establish and enforce strong access restrictions to mitigate the risk of unauthorised access.

It is recommended to do privacy impact assessments to detect and address any privacy concerns and to assure adherence to legislative requirements.

Ensure that users provide unequivocal permission to process their data, and enable them to exercise their rights to access, alter, or delete their data as required.

Incorporating Privacy by Design principles is essential in developing and implementing intelligent transit applications that rely on cloud-based technology. Transportation authorities and cloud service providers can foster user confidence, preserve sensitive data, and comply with ethical and legal data protection standards by incorporating privacy concerns. Privacy by Design grants people more agency in managing their data while guaranteeing that intelligent transport advancements contribute to a digital environment that prioritises security and respects privacy. Privacy Impact Assessments (PIAs) do not possess an intrinsic mathematical nature; they include methodical evaluations of possible privacy hazards. Quantitative analysis encompasses the assessment of the potential consequences arising from a privacy breach, specifically about factors such as the sensitivity of the compromised data, the level of confidence placed by users, and the fines imposed by regulatory bodies. Risk quantification is not only reliant on mathematical methods. The process of risk assessment and quantification may include the assignment of numerical values to prospective privacy threats. This may facilitate prioritising mitigation solutions by considering their possible effect and probability. The usability and user experience analysis is not only based on mathematical principles. In reality, user experience evaluation may include quantitative measures such as user satisfaction ratings, interaction durations, and job completion rates. These metrics serve the purpose of ensuring that privacy-enhancing technologies do not impede the overall user experience. Privacy effect measurements are not exclusively based on mathematical principles. Developing privacy impact metrics may include establishing quantitative indicators of privacy safeguarding, such as quantifying the anonymity attained via anonymization methods. Consent Management and Compliance Metrics involve using quantitative analysis to evaluate the efficacy of user consent methods and the level of adherence to regulatory requirements shown by privacy policies.

Data Minimization Metrics refers to a mathematical approach that enables the measurement of the extent to which data exposure is reduced via data minimization measures. This analysis aids in striking a balance between the usefulness of data and safeguarding privacy. Privacy-preserving analytics refers to data analysis while protecting individuals' privacy. The evaluation of privacy-preserving analytics techniques encompasses more than just mathematical considerations. It entails a comprehensive assessment of their performance, including quantitatively comparing the accuracy and insights obtained from analysing raw data with those acquired from analysing privacy-protected data. The administration of encryption keys encompasses more than just mathematical aspects. It includes implementing safe mathematical concepts, such as crucial creation, distribution, and rotation.

Access control metrics are not only based on mathematical principles. Evaluating the efficacy of access controls may include assessing the frequency of unauthorised access attempts and successful breaches. The rates at which individuals actively consent to a specific action or process. The quantification of the proportion of users who voluntarily participate in data processing activities might provide valuable information about their inclination to contribute data and their level of confidence in the privacy safeguards implemented by the system. The study titled "Quantifying the Effects of Privacy Enhancements on System Performance" presents a mathematical framework that may be used to assess the influence of various privacy-enhancing protocols on the

operational efficiency of intelligent transportation systems. This analysis encompasses processing speed, storage demands, and computational overhead. Privacy by design emphasises principles and holistic considerations. At the same time, the practical implementation and evaluation of privacy-preserving mechanisms and user experiences may involve quantitative analysis, metrics, and the application of mathematical concepts to address specific aspects of privacy protection.

7.6. Data Governance and Compliance. Cloud platforms frequently provide data governance and compliance management tools and frameworks. These tools enable organisations to define data retention policies, consent management mechanisms, and data access audit trails to maintain regulatory compliance, such as GDPR or CCPA [30], as cloud-based solutions continue to transform intelligent transportation applications, data governance and compliance become of utmost importance [10]. Data governance incorporates the procedures, policies, and guidelines that prescribe how data is managed, accessed, and protected. In contrast, compliance is the observance of applicable laws, regulations, and industry standards governing data privacy and security. Robust data governance frameworks and compliance measures are necessary to ensure ethical and legal practices in cloud-based intelligent transportation applications. Delineating data ownership and designating data management responsibilities within a cloud-based infrastructure ensures accountability and adequate handling of sensitive data. Implementing measures to maintain data accuracy, consistency, and integrity ensures the dependability of the data used in decision-making and research. Developing data collection, storage, retention, and disposition policies reduces the risk of unauthorised access or data breaches by ensuring that data is handled appropriately throughout its lifecycle. Categorising data according to its level of sensitivity enables the application of appropriate security controls and access restrictions, thereby ensuring that sensitive data is adequately protected. When dealing with personally identifiable information (PII) in intelligent transportation applications, compliance with data privacy laws such as the General Data Protection Regulation (GDPR) in Europe or the California Consumer Privacy Act (CCPA) in the United States is crucial [24]. Effective encryption methods, such as Transport Layer Security (TLS), during data transmission between cloud servers and end users serves as a protective measure against possible eavesdropping and interception of data.

The implementation of optimal security practises may be effectively facilitated by adhering to industry-specific standards, such as ISO 27001 for information security management or the NIST Cybersecurity Framework [32]. Conducting Privacy Impact Assessments (PIAs) aids in the identification and mitigation of privacy risks linked to data processing operations, hence assuring the proactive resolution of privacy problems. The regular implementation of internal and external compliance audits serves to assess the effectiveness of data governance practises and suggest areas for improvement. Establishing formal agreements to delineate the rights, obligations, and security prerequisites regarding data use is essential while engaging in collaborations with third-party businesses or exchanging data across diverse parties. Before sharing or doing analysis, it is common practice to anonymize or pseudonymize sensitive data to protect the identity of individuals and mitigate any privacy hazards.

The implementation of data governance and compliance measures is vital to preserve data integrity, protect users' privacy, and guarantee the ethical utilisation of cloud solutions within intelligent transportation systems. Transportation authorities and cloud service providers can cultivate user trust, stimulate innovation, and establish a secure and sustainable smart transportation ecosystem by implementing robust data governance frameworks, complying with relevant data privacy regulations, and embracing secure data-sharing practices. To fully harness the capabilities of cloud-based solutions within the dynamic transportation industry, it is imperative to prioritise the ethical and legal dimensions of data management, focusing on safeguarding data and privacy. Risk assessment and quantification is a multidimensional process that extends beyond quantitative considerations. In addition to numerical analysis, risk assessment includes the evaluation of the possible consequences and probability associated with non-compliance with data protection standards. Quantitative analysis may be utilised to evaluate regulatory fines' financial and reputational repercussions. The audit trail analytical process involves examining data access and alterations, using mathematical, and analytical techniques to identify patterns of unauthorised access, probable breaches, or irregularities in data use.

The mathematical study known as the Data Classification and Sensitivity study is used to assess the sensitivity of various data kinds and establish suitable security measures by their respective levels of secrecy. The measurement of possible privacy risks found in Privacy Impact Assessments (PIAs) may include quantitative

evaluation of the probability and consequences of various hazards. The analysis of data retention periods aims to identify the most efficient duration for storing data, considering both regulatory compliance and storage costs. This process often involves using mathematical models that examine many elements, such as patterns of data consumption, legal obligations, and expenditures associated with data storage. The performance metrics used in compliance audits assess the effectiveness of these audits in finding gaps and possible breaches. These metrics primarily rely on quantitative measures such as audit coverage, detection rates, and the occurrence of false positives and negatives. The present study focuses on doing a quantitative analysis of consent management. The process of assessing user opt-in rates and monitoring user preferences for data processing includes the quantitative examination of user activity. The evaluation of anonymization methods involves using quantitative measures to determine the protection of identity and preservation of data usefulness. These metrics are not only based on mathematical principles. The Quantitative Assessment of Data Sharing Agreements involves the evaluation of security standards and duties included in formal agreements for sharing data. This assessment may consist of using mathematical techniques to compare different security measures. Compliance Score Metrics provides a metric that measures the degree to which an application conforms to relevant norms and standards. This process may include giving numerical values to various compliance criteria. The topic of concern is the accuracy and consistency of data. Metrics are used to measure the precision and reliability of data during its entire lifespan, and they may impact mathematical analysis and the ability to compare data against predetermined standards.

Although not all components of data governance and compliance are inherently rooted in mathematical principles, the use of quantitative analysis, metrics, and modelling may facilitate the evaluation of various measures' risks, effects, and efficacy. These factors may assist in making well-informed judgements on data management and compliance techniques in cloud-based intelligent transportation apps.

8. Cloud-Based Solutions For Intelligent Transportation Applications. Technology development has revolutionised numerous industries, including transportation. Intelligent Transportation Systems (ITS) employ cutting-edge technologies to improve transportation's efficacy, safety, and sustainability [9]. Cloud-based solutions have emerged as a crucial enabler for the implementation and success of these intelligent transportation applications. This article will examine the advantages, difficulties, and prospective applications of cloud-based solutions in intelligent transit. The infrastructure of cloud-based solutions is elastic and can scale resources up or down based on demand. This is especially essential for transportation systems with fluctuating loads, such as traffic management during rush hour or peak season [19].

Platforms in the cloud enable the seamless accumulation, processing, and analysis of enormous quantities of real-time data from various sources, such as GPS, sensors, and cameras. This information can optimise traffic flow, monitor road conditions, and provide travellers with current information [29]. Using a cloud-based strategy, transport authorities can reduce infrastructure expenditures because they no longer need to invest substantially in on-premises hardware and maintenance [33]. In addition, cloud services offer pay-as-you-go pricing models, allowing businesses to pay only for the resources they consume [38]. Cloud solutions facilitate data sharing and collaboration between parties, such as government agencies, transportation providers, and third-party developers. This interoperability encourages the development of innovative applications that can solve complex transportation issues. Cloud platforms enable sophisticated traffic management systems that use real-time data analysis to optimise signal timing, control traffic flow, and reduce congestion. These solutions can result in reduced travel durations and enhanced traffic efficiency overall. In Vehicle-to-Everything (V2X) communication, cloud-based solutions facilitate data transmission between vehicles, infrastructure, and other devices.This technology improves road safety by alerting drivers in real-time to potential road hazards and enhancing their situational awareness.

Public transportation routes, schedules, and fleet management can be optimised using cloud-based analytics. This results in enhanced passenger experiences, decreased operational expenses, and increased public transportation utilisation [2]. Connected parking systems in the cloud can direct drivers to available parking spaces, thereby reducing traffic congestion and emissions caused by drivers browsing for parking. Cloud-based predictive maintenance applications utilise sensor data from vehicles and infrastructure to determine maintenance needs. This proactive strategy improves maintenance planning, decreases idleness, and increases the overall dependability of conveyance systems. Cloud-based solutions require adequate security measures to

protect sensitive transportation data from unauthorised access and cyber threats.

As transport systems significantly rely on real-time data, cloud service providers must ensure high availability and redundancy to prevent disruptions. Cloud-based solutions rely on dependable internet connectivity and minimal latency, which can be difficult in remote or underdeveloped areas. When utilising cloud-based services, transportation authorities must comply with applicable data protection and privacy regulations. The advantages of cloud-based solutions for intelligent transportation applications range from increased scalability and real-time data processing to cost savings and collaboration opportunities. By addressing potential obstacles and employing best practices, transportation authorities can unlock the full potential of cloud-based technologies and promote innovation in the intelligent transportation sector, resulting in a safer, more efficient, and more sustainable transportation network. Scalability Analysis is a mathematical model that can be used to analyze the scalability of cloud-based solutions, considering factors like resource utilization, response times, and costs as the system scales up or down. Resource Allocation Optimization is a mathematical optimization technique that can help determine the optimal allocation of resources within a cloud-based transportation system to ensure efficient data processing and analysis. Real-Time Data Processing is a Mathematical algorithm, and models may be employed to process real-time data efficiently, considering factors like data arrival rates, processing speeds, and latency.

Traffic Flow Optimization is a mathematical simulation or model that can optimize traffic flow based on real-time data, aiming to reduce congestion and travel times. Predictive Analytics is a mathematical technique such as regression analysis or machine learning that can be applied to predict future transportation patterns, helping in proactive decision-making. The article discusses the benefits of cloud-based solutions regarding cost savings and improved efficiency. Mathematical metrics could quantify these improvements in percentages, ratios, or other quantitative measures. Mathematical analysis might be used to assess network latency and its impact on real-time data processing in the context of reliable data transmission. Data Sharing Efficiency is a Mathematical model that could be used to assess the efficiency of data sharing and collaboration among different parties, considering factors like data exchange rates and data integrity. Privacy and Data Protection Metrics are quantitative metrics that could be used to assess the level of privacy protection achieved through cloud-based solutions, considering factors like data anonymization effectiveness and compliance with privacy regulations. Cost-benefit analysis is a mathematical analysis that can be employed to perform a cost-benefit analysis of adopting cloud-based solutions, considering both the costs of implementation and the potential benefits of efficiency, scalability, and user satisfaction. Risk Assessment and Mitigation is a mathematical analysis that might assess potential risks associated with cloud-based solutions, quantifying the likelihood and potential impact of disruptions or security breaches. While the content in the text emphasizes the operational and technological aspects of cloud-based solutions, integrating relevant mathematical analyses or models can enhance the depth and precision of the discussion in areas such as optimization, scalability, efficiency, and risk assessment.

Enhanced Efficiency. Existing knowledge of cloud-based solutions highlights their ability to improve the efficiency of intelligent transportation systems by providing real-time data processing, traffic management, and decision-making capabilities.

Scalability. Cloud computing allows transportation systems to scale resources based on demand, effectively accommodating fluctuating traffic volumes and user requirements.

Cost Savings. Adopting cloud-based solutions can reduce infrastructure and maintenance costs, as organizations can leverage the cloud provider's resources instead of investing in expensive on-premises hardware.

Data Accessibility. Cloud-based platforms enable seamless data sharing and collaboration among stakeholders, promoting data-driven decision-making and improved transportation services.

Innovation and Flexibility. Cloud solutions foster an environment for innovation and experimentation, allowing developers to create and deploy new intelligent transportation applications quickly.

9. Drawbacks of Existing Knowledge on Cloud-based Solutions for Intelligent Transportation.

Data Security and Privacy Concerns. Cloud computing introduces security and privacy risks, as transportation data is stored and processed off-site. Breaches or unauthorized access to cloud-stored data can compromise user privacy and lead to data breaches.

Reliability and Downtime. Cloud-based solutions rely on internet connectivity, and downtime or disruptions in internet services can affect the availability and performance of intelligent transportation applications.

Data Residency and Compliance. Cloud services might operate across different jurisdictions, leading to challenges in ensuring data residency compliance and adhering to relevant data protection laws.

Dependency on Cloud Providers. Organizations relying heavily on cloud-based solutions may face vendor lock-in, making it challenging to switch providers or migrate data if needed.

Network Latency. For real-time applications, network latency can affect the responsiveness of cloud-based systems, potentially impacting the overall performance of intelligent transportation applications.

Complexity of Integration. Integrating existing transportation infrastructure with cloud-based solutions may be complex and require careful planning to avoid disruptions during the migration process. Existing knowledge of cloud-based solutions for intelligent transportation showcases numerous advantages, such as enhanced efficiency, scalability, cost savings, data accessibility, and opportunities for innovation. However, it acknowledges significant drawbacks, including data security and privacy concerns, reliability issues, compliance challenges, vendor lock-in, network latency, and integration complexities. Addressing these drawbacks is crucial for the responsible and successful adoption of cloud-based solutions, ensuring that data and privacy are protected while reaping the benefits of cloud computing in the intelligent transportation domain.

10. Case Study. Cloud-based solutions have revolutionised intelligent transportation, which offers increased efficiency and connectivity. However, the increased use of cloud computing has raised significant data security and privacy concerns. This paper presents a series of case studies and illustrations to illuminate the real-world implications and efficacy of cloud-based security measures in intelligent transportation. These case studies emphasise organisations' challenges and practical implementation strategies, providing valuable insights into data protection in this dynamic domain.

10.1. Case Study 1: Citywide Traffic Management System.

Scenario. A thriving city implements a municipal cloud-based traffic management system to optimise traffic flow, reduce congestion, and improve public safety.

Challenges.

Data Privacy. The system accumulates voluminous data from traffic cameras, GPS devices, and connected vehicles, raising privacy and anonymity concerns.

Data Security. Protecting real-time traffic data and system integrity against cyber threats and potential hijacking attempts is crucial for preventing disruptions and ensuring public safety.

Implementation Strategies.

Anonymization. To ensure individual vehicles' and pedestrians' privacy, the city employs sophisticated anonymization techniques that aggregate and conceal personal data to protect user identities.

Secure Data Transmission. Using robust encryption protocols for data in transit ensures the confidentiality and integrity of data transmitted between the cloud platform and connected devices.

Results. While addressing data privacy concerns, the cloud-based traffic management system optimises traffic flow, reduces congestion, and enhances public safety in general. The anonymization techniques and secure data transmission safeguard user privacy and prevent unauthorised access to sensitive information.

10.2. Case Study 2: Smart Public Transportation System. Scenario: A sophisticated public transport system employs cloud-based solutions to optimise bus and railway routes, schedules, and fleet management.

Challenges.

- Data Residency: Concerning the physical location of data stored in the cloud and assuring conformance with data residency regulations, the transport authority confronts challenges.
- Proprietorship Concerns: The authority must clarify data possession and control, ensuring that an agency's transportation retains power over the data.

Implementation Strategies.

- Data Governance: The transportation authority implements a robust data governance framework to define data ownership, storage, and access policies, ensuring data residency requirements are met.
- Transparent Agreements: The transport authority establishes clear agreements with the cloud service provider regarding data custody and control, granting it full administrative rights over its data.

Results. By addressing concerns regarding data residency and ownership, the intelligent public transport system obtains the confidence of stakeholders and ensures compliance with applicable regulations. The effective cloud-based solution optimises conveyance services, enhancing passenger satisfaction and decreasing operational expenses. Case studies and real-world examples illustrate the practical implications of cloud-based security measures in intelligent transportation applications. Cloud-based solutions are indispensable for optimising transportation systems and protecting sensitive data by addressing data privacy, security, and ownership challenges. These examples provide transportation authorities, industry stakeholders, and policymakers with valuable guidance towards adopting cloud-based solutions responsibly and securely while safeguarding data and privacy in intelligent transportation.

11. Discussion. The discussion section emphasises the most important considerations and strategies for data and privacy protection in cloud-based intelligent transportation applications. It examines the role of cloud computing in addressing data security and privacy issues, but it is crucial to evaluate the efficacy and limitations of these solutions.

While encryption and access control mechanisms provided by cloud platforms can improve data security, it is essential to observe that encryption alone does not provide absolute security. Encryption algorithms have occasionally been compromised or inadequately implemented, resulting in data intrusions. In addition, access control mechanisms are only effective if they are appropriately configured and managed, as missed configurations or vulnerabilities can result in unauthorised access.

There are disadvantages to cloud storage and backup solutions for data protection. Organisations must choose cloud service providers with a strong security focus and robust data protection measures with care. Concerns persist regarding data residency and proprietorship, as organisations may have limited control over the physical location of their data and the permissions to access and administer it.

Even though cloud platforms provide threat detection and intrusion prevention measures, it is essential to recognise that these systems are not infallible. Complex cyber attacks can still circumvent detection mechanisms, and new vulnerabilities may emerge as technologies evolve. Continuous monitoring, regular updates, and proactive security measures are essential to remain abreast of evolving threats. The protection of privacy in cloud-based intelligent transportation applications is a challenging problem. Although anonymisation and pseudonymisation techniques can aid in protecting user identities, it is essential to recognise that re-identification attacks and privacy breaches can still occur. Privacy by design principles are crucial, but their successful implementation requires a comprehensive understanding of privacy risks and impact assessments.

Cloud platforms' data governance and compliance frameworks can aid organisations in meeting regulatory requirements. However, organisations must also be accountable for comprehending and abiding by applicable data protection laws and regulations. Compliance should not rely solely on cloud service providers because organisations are ultimately responsible for the security and confidentiality of their data. In intelligent transportation applications, it is essential to recognise cloud-based solutions' potential obstacles and limitations for data security and privacy. Organisations must thoroughly evaluate the risks and benefits of these obstacles. Adopting a comprehensive approach to security that incorporates many levels of protection, frequent audits, and continuing training is suggested to limit risks and preserve the integrity and privacy of data.

Even though cloud-based solutions provide beneficial security and privacy features, they are not fail-safe. In intelligent transportation applications, organisations must exercise caution and implement additional safeguards

to address the limitations and potential risks associated with cloud computing. Continuous evaluation, proactive security measures, and comprehensive security strategies are essential for sustaining data security and privacy in a constantly changing environment. Several limitations were encountered during the research for "Protecting Data and Privacy: Cloud-based Solutions for Intelligent Transportation," which affected the study's scope and findings. Data availability complicated access to exhaustive and up-to-date information on real-world cloud-based intelligent transportation implementations, potentially resulting in data gaps. Despite the systematic approach, the extensive literature on data security, privacy, and cloud-based solutions in smart transportation made it difficult to identify all relevant studies, resulting in unintentional omissions. In addition, the analysis was incomplete due to cloud service providers' limited disclosure of security measures.

Due to the rapid evolution of cloud computing and intelligent transportation systems, it was possible that new advancements would emerge during research that could not be completely incorporated. When discussing real-world case studies or industry-specific implementations, the amount of specific information that could be disclosed was also influenced by ethical considerations surrounding data privacy and confidentiality.

Investigating the implementation challenges organisations face when deploying cloud-based solutions, conducting a comparative analysis of the security features of different cloud service providers, and understanding user perceptions and acceptance of data security and privacy in intelligent transportation applications are examples of research gaps and areas for further investigation. In addition to examining the challenges of complying with data protection regulations across jurisdictions and international privacy frameworks, it is vital to conduct long-term assessments of cloud-based security measures and their effectiveness over extended periods.

Addressing these research voids will contribute to a deeper comprehension of data security and privacy in cloud-based intelligent transportation, allowing for more informed decision-making and developing robust security strategies in this swiftly evolving field. It will also pave the way for enhancing user confidence, data security, and the development of intelligent transportation applications over time.

12. Conclusion. As intelligent transportation systems continue to evolve, it becomes increasingly important to protect the security and privacy of data. Cloud-based solutions provide a robust framework for effectively addressing these concerns. Organizations can protect sensitive data and safeguard user privacy by implementing encryption, access controls, threat detection mechanisms, and privacy protection measures. Adopting these cloud-based solutions will facilitate the extensive adoption of intelligent transportation applications while infusing users and stakeholders with confidence.

REFERENCES

[1] Abd-El-Atty, B., Iliyasu, A. M., Alaskar, H., Abd El-Latif, A. A. (2020). A robust quasi-quantum walks-based steganography protocol for secure transmission of images on cloud-based E-healthcare platforms. *Sensors*, 20(11), 3108.

[2] Alam, T. (2021). Cloud-based IoT applications and their roles in smart cities. *Smart Cities*, 4(3), 1196-1219

[3] Alkhariji, L., De, S., Rana, O., and Perera, C. (2023). Semantics-based privacy by design for Internet of Things applications. *Future Generation Computer Systems*, 138, 280-295.

[4] Butpheng, C., Yeh, K. H., Xiong, H. (2020). Security and privacy in IoT-cloud-based e-health systems—A comprehensive review. *Symmetry*, 12(7), 1191.

[5] Cavoukian, A. (2010). Privacy by design: the definitive workshop. *Identity in the Information Society*, 3(2), 247-251.

[6] Cheng, L., Liu, F., Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 7(5), e1211.

[7] Conte, R., Sansone, F., Tonacci, A., Pala, A. P. (2022). Privacy-by-Design and Minimization within a Small Electronic Health Record: The Health360 Case Study. *Applied Sciences*, 12(17), 8441

[8] Das, D., Banerjee, S., Chatterjee, P., Ghosh, U., Biswas, U. (2023). Blockchain for Intelligent Transportation Systems: Applications, Challenges, and Opportunities. *IEEE Internet of Things Journal*.

[9] Gholamhosseinian, A., and Seitz, J. (2021). Vehicle classification in intelligent transport systems: An overview, methods and software perspective. *IEEE Open Journal of Intelligent Transportation Systems*, 2, 173-194

[10] Gohar, A., and Nencioni, G. (2021). The role of 5G technologies in a smart city: The case for intelligent transportation system. *Sustainability*, 13(9), 5188.

[11] Guerrero-Ibanez, J. A., Zeadally, S., Contreras-Castillo, J. (2015). Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and internet of things technologies. *IEEE Wireless Communications*, 22(6), 122-128.

[12] Gunduz, M. Z., Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer Networks*, 169, 107094.

[13] Haque, A. B., Bhushan, B., Dhiman, G. (2022). Conceptualising smart city applications: Requirements, architecture, security issues, and emerging trends. *Expert Systems*, 39(5), e12753.
[14] Hon, W. K., Millard, C., Walden, I. (2011). The problem of 'personal data'in cloud computing: what information is regulated?—the cloud of unknowing. *International Data Privacy Law*, 1(4), 211-228.
[15] Hoofnagle, C. J., Van Der Sloot, B., Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. *Information Communications Technology Law*, 28(1), 65-98.
[16] Hussain, M. M., Alam, M. S., Beg, M. S. (2019). Fog computing model for evolving smart transportation applications. *Fog and Edge Computing: Principles and Paradigms*, 22(4), 347-372.
[17] Joshi, J. B., Bertino, E., Latif, U., Ghafoor, A. (2005). A generalized temporal role-based access control model. *IEEE transactions on knowledge and data engineering*, 17(1), 4-23
[18] Kaluarachchi, Y. (2022). Implementing data-driven smart city applications for future cities. *Smart Cities*, 5(2), 455-474.
[19] Latha, V. P., Reddy, N. S., Babu, A. S. (2023). Optimizing Scalability and Availability of Cloud Based Software Services Using Modified Scale Rate Limiting Algorithm. *Theoretical Computer Science*, 943, 230-240.
[20] Lee, I., Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, 58(4), 431-440.
[21] Masud, M., Gaba, G. S., Choudhary, K., Alroobaea, R., Hossain, M. S. (2021). A robust and lightweight secure access scheme for cloud based E-healthcare services. *Peer-to-peer Networking and Applications*, 14(5), 3043-3057.
[22] Mehta, P., Gupta, R., Tanwar, S. (2020). Blockchain envisioned UAV networks: Challenges, solutions, and comparisons. *Computer Communications*, 151, 518-538.
[23] Mollah, M. B., Zhao, J., Niyato, D., Guan, Y. L., Yuen, C., Sun, S. et al (2020). Blockchain for the internet of vehicles towards intelligent transportation systems: A survey. *IEEE Internet of Things Journal*, 8(6), 4157-4185.
[24] Mueller, S., Taylor, C. R., Mueller, B. (2022). *Managing change related to consumer privacy laws: targeting and personal data use in a more regulated environment*. In Media and Change Management Creating a Path for New Content Formats, Business Models, Consumer Roles, and Business Responsibility. Cham Springer International Publishing
[25] Narwal, P., Duhan, N., Bhatia, K. K. (2022). Image Systems and Visualisations 3. *Multimedia Computing Systems and Virtual Reality*, 45-78.
[26] Oprescu, A. M., Mir´o-Amarante, G., García-Díaz, L., Rey, V. E., Chimenea-Toscano, A., MartínezMartínez, R., Romero-Ternero, M. C. (2022). Towards a data collection methodology for Responsible Artificial Intelligence in health: A prospective and qualitative study in pregnancy. *Information Fusion*, 83, 53-78.
[27] Pandeeswari, N., Kumar, G. (2016). Anomaly detection system in cloud environment using fuzzy clustering based ANN. *Mobile Networks and Applications*, 21, 494-505.
[28] Patel, A., Taghavi, M., Bakhtiyari, K., Júnior, J. C. (2013). An intrusion detection and prevention system in cloud computing: A systematic review. *Journal of Network and Computer Applications*, 36(1), 25-41.
[29] Pérez, J., Léon, J., Castilla, Y., Shahrabadi, S., Anjos, V., Ad˜ao, T., et al (2023). A cloud-based 3D real-time inspection platform for industry: a case-study focusing automotive cast iron parts. *Procedia Computer Science*, 219, 339-344
[30] Ranchal, R., Bastide, P., Wang, X., Gkoulalas-Divanis, A., Mehra, M., Bakthavachalam, S., et al (2020). Disrupting healthcare silos: Addressing data volume, velocity and variety with a cloud-native healthcare data ingestion service. *IEEE Journal of Biomedical and Health Informatics*, 24(11), 3182-3188.
[31] Rimal, B. P., Jukan, A., Katsaros, D., Goeleven, Y. (2011). Architectural requirements for cloud computing systems: an enterprise cloud approach. *Journal of Grid Computing*, 9, 3-26.
[32] Roy, P. P. (2020). A high-level comparison between the nist cyber security framework and the iso 27001 information security standard. In *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications* (NCETSTEA) (pp. 1-3). IEEE.
[33] Saranya, N., Sakthivadivel, M., Karthikeyan, G., Rajkumar, R. (2023). Securing the Cloud: An Empirical Study on Best Practices for Ensuring Data Privacy and Protection. *International Journal of Engineering and Management Research*, 13(2), 46-49
[34] Semantha, F. H., Azam, S., Yeo, K. C., Shanmugam, B. (2020). A systematic literature review on privacy by design in the healthcare sector. *Electronics*, 9(3), 452.
[35] Singh, B., Gupta, A. (2015). Recent trends in intelligent transportation systems: a review. *Journal of Transport Literature*, 9, 30-34.
[36] Sood, S. K. (2021). Smart vehicular traffic management: An edge cloud centric IoT based framework. *Internet of Things*, 14, 100140.
[37] Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., Shen, X. (2022). A survey on metaverse: Fundamentals, security, and privacy. *IEEE Communications Surveys Tutorials*
[38] Zhao, S., Miao, J., Zhao, J., Naghshbandi, N. (2023). A comprehensive and systematic review of the banking systems based on pay-as-you-go payment fashion and cloud computing in the pandemic era. *Information Systems and e-Business Management*, 1-29

Edited by: Zhenling Liu
Special Issue on: Cloud Computing for Intelligent Traffic Management and Control
Received: Jun 30, 2023
Accepted: Aug 21, 2023