International Journal of Basic and Applied Sciences, 15 (1) (2026) 148-160

International Journal of Basic and Applied Sciences

Website: www.sciencepubco.com/index.php/IJBAS
https://doi.org/10.14419/4ve8yy06
Research paper



A Blockchain-Enabled Framework for Privacy Preserving Smart Mobility Services

Hani Al-Balasmeh [1] *, Fayzeh Abdulkareem Jaber [2], Sa'eed Serwan Abdulsattar [3]

[1] *Dept. of Informatics Engineering, University of Technology Bahrain*
[2] *Dept of Computer Studies, University of Technology Bahrain*
[3] *Dept of Electrical and Electronics Engineering, University of Bahrain*
**Corresponding author E-mail: h.albalasmeh@utb.edu.bh*

Received: December 31, 2025, Accepted: January 24, 2026, Published: January 26, 2026

Abstract

Smart mobility services generate large volumes of sensitive location and identity data, raising critical concerns related to privacy leakage, security vulnerabilities, and trust in large-scale urban deployments. To address these challenges, this paper proposes a blockchain-based privacy-preserving framework for smart mobility services that integrates geo-indistinguishability, pseudonymous authentication, Zero-Knowledge Proofs (ZKPs), and Proof-of-Authority (PoA) consensus into a unified architecture. The framework ensures end-to-end privacy by combining calibrated location obfuscation with decentralized transaction validation and immutable auditability, thereby mitigating both inference-based attacks and reliance on centralized trust.

The proposed framework was evaluated using the TAPAS Cologne mobility dataset, comprising 1,000 simulated vehicles and 20 blockchain validators. Experimental results demonstrate that adversarial inference accuracy is reduced to below 12%, while approximately 75% navigation utility is preserved at balanced privacy budgets. Security analysis confirms robust protection against tracking, replay, Sybil, and collusion attacks, with replay attack success rates reduced from 70% to 2% through the enforcement of timestamps and nonces, along with cryptographic verification.

Performance evaluation demonstrates that the framework achieves high throughput (1,200 transactions per second) with sub-second latency (0.8 seconds) under realistic transaction loads. Storage growth is optimized to 2.1 GB per million transactions, and the PoA consensus mechanism achieves approximately 30% lower energy consumption compared to Proof-of-Stake-based designs. In addition, resilience experiments confirm Byzantine fault tolerance under up to 30% malicious validator participation, without service degradation.

Overall, the results demonstrate the practical feasibility of deploying the proposed framework in real-world smart mobility ecosystems that require simultaneous privacy preservation, scalability, and energy efficiency. The framework represents a significant step toward trustworthy, privacy-aware, and sustainable smart-city mobility infrastructure, providing a robust foundation for next-generation decentralized mobility services.

Keywords: *Blockchain; Privacy Preservation; Geo-indistinguishability; Smart Mobility; Vehicular Networks; Zero-Knowledge Proofs; Proof-of-Authority; Energy Efficiency; Cybersecurity; Smart Cities.*

1. Introduction

The rapid expansion of smart mobility services—such as ride-sharing, e-ticketing, and real-time navigation—has resulted in the continuous generation of large volumes of fine-grained location and identity data. While these services significantly improve urban efficiency, accessibility, and sustainability, they simultaneously introduce serious privacy and security challenges. Sensitive data, including vehicle trajectories, spatiotemporal movement patterns, and user identifiers, can be exploited through tracking, profiling, and inference attacks, thereby undermining user trust and regulatory compliance in smart city ecosystems [1], [2].

Early attempts to mitigate privacy risks in mobility systems primarily relied on location obfuscation techniques, including the generation of dummy locations and trajectory distortion [3]. These approaches successfully reduced adversarial inference accuracy by introducing uncertainty into location traces. However, they were implemented mainly within centralized architectures, making them vulnerable to single points of failure, insider attacks, and limited transparency. Moreover, centralized trust models lack verifiable auditability, a requirement that is increasingly necessary in multi-stakeholder smart mobility environments.

More recent research has explored blockchain-enabled mobility frameworks to address concerns about trust, integrity, and accountability through decentralization and immutable ledgers [4], [5]. Blockchain-based approaches have demonstrated effectiveness in preventing data tampering and enabling transparent service coordination across mobility providers. Nevertheless, many existing solutions prioritize transparency and scalability over fine-grained location privacy. Since blockchain ledgers are inherently append-only and observable by validators, naïve integration can inadvertently expose mobility patterns and enable re-identification attacks.

Copyright © Hani Al-Balasmeh et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

To address these limitations, this paper proposes a blockchain-based privacy-preserving smart mobility framework that unifies location privacy mechanisms, cryptographic authentication, and decentralized trust into a cohesive system. Building upon the dummy-location privacy model introduced in prior work [3], the proposed framework integrates geo-indistinguishability, pseudonymous authentication, Zero-Knowledge Proofs (ZKPs), and a Proof-of-Authority (PoA) consensus mechanism. This integration enables end-to-end privacy preservation while maintaining low latency and high throughput, making it suitable for real-time mobility services.

Fig. 1 illustrates the high-level architecture of the proposed system, structured into three tightly coupled layers: the User and IoT Layer, the Blockchain and Privacy Layer, and the Application Layer. At the user side, raw GPS coordinates and service requests are transformed using algorithmic location privacy mechanisms before transmission. At the blockchain layer, smart contracts enforce authentication, access control, and transaction validation, while PoA consensus ensures efficient and energy-aware block finalization. The application layer delivers mobility services without direct access to sensitive identity or precise location data.

A key contribution of the framework lies in its algorithm-driven enforcement of privacy. As shown in Fig. 2, user authentication is performed using a pseudonym generation algorithm combined with Zero-Knowledge Proof–based eligibility verification. This approach allows users to prove authorization without revealing real identities or long-term identifiers, thereby preventing identity linkage across service sessions. Pseudonyms are periodically refreshed using time-based and nonce-based algorithms, further reducing the risk of correlation.

Location privacy is enforced through a combination of geo-indistinguishability and dummy-location synthesis, as illustrated in Fig. 3. An algorithmic noise-injection mechanism based on the planar Laplace distribution ensures that the probability of distinguishing between nearby locations is mathematically bounded. This is complemented by a dummy-generation algorithm that produces multiple plausible locations, reducing the probability of adversarial success to near-random guessing. Unlike heuristic obfuscation methods, these algorithms provide formal privacy guarantees while preserving acceptable navigation utility.

The framework is evaluated using the TAPAS Cologne mobility dataset, comprising 1,000 vehicles and 20 blockchain validators. Experimental results show that adversarial inference accuracy drops below 12%, while replay attack success rates decrease from 70% to 2%. Despite vigorous privacy enforcement, the system maintains a throughput of 1,200 transactions per second with sub-second latency. Compared to existing blockchain-based mobility solutions, the proposed approach achieves superior privacy protection while reducing storage growth and energy consumption by approximately 30% [4], [5]. These results confirm the practicality and scalability of the proposed design for real-world smart city deployments.

The main contributions of this paper are summarized as follows:

1) A unified privacy-preserving smart mobility framework that integrates dummy-location obfuscation, geo-indistinguishability, Zero-Knowledge Proofs, and blockchain consensus.
2) Algorithmic authentication and location privacy mechanisms that ensure unlinkability, resistance to inference attacks, and formal privacy guarantees.
3) A comprehensive security evaluation demonstrating resilience against tracking, replay, Sybil, and collusion attacks.
4) An extensive performance evaluation confirming low latency, high throughput, and reduced energy consumption suitable for large-scale urban mobility systems.
5) A systematic evolution of prior dummy-based privacy research into a scalable, blockchain-enabled ecosystem for next-generation smart cities.

The remainder of this paper is organized as follows. Section II reviews related work. Section III presents the system architecture in detail. Section IV describes the proposed framework and associated algorithms. Section V evaluates the results of privacy, security, and performance. Section VI discusses practical implications and limitations, and Section VII concludes the paper.

2. Literature Review

Research on privacy-preserving smart mobility services has evolved rapidly in response to the growing deployment of location-aware urban applications. Existing work can be broadly categorized into three main research streams: (i) vehicular and IoT privacy frameworks, (ii) blockchain-based trust and data integrity frameworks, and (iii) advanced cryptographic and hybrid privacy-preserving approaches. While each stream addresses specific aspects of mobility privacy and security, their individual limitations motivate the need for an integrated framework that jointly considers decentralization, fine-grained location privacy, and system scalability.

2.1. Vehicular and IoT privacy frameworks

Early research on smart mobility privacy primarily focused on Vehicular Cloud Networks (VCNs) and IoT-enabled transportation systems. These approaches typically rely on anonymization, trajectory obfuscation, and the generation of dummy locations to reduce the risk of user re-identification and tracking attacks. Such mechanisms aim to conceal real mobility patterns by introducing uncertainty into spatiotemporal data streams.

Al-Balasmeh et al. proposed anonymization and location obfuscation mechanisms to mitigate inference attacks targeting vehicular trajectories [3]. Building on this work, the TIET-GEO framework introduced geofence-based dummy location generation to enhance privacy in IoT mobility services [4]. This approach demonstrated improved resistance to location-correlation attacks by dynamically generating plausible alternative positions within predefined geographic boundaries. A subsequent extension incorporated RSA-based encryption and token-based communication to secure real-time GPS data transmission in vehicular cloud environments [5].

Despite their effectiveness in reducing direct privacy leakage, these frameworks rely heavily on centralized architectures, where trusted servers perform data aggregation, verification, and access control. Such centralization introduces several inherent weaknesses, including single points of failure, susceptibility to insider threats, limited scalability under high vehicular density, and reduced transparency for users and service providers. These limitations significantly constrain the applicability of purely centralized privacy mechanisms in large-scale, multi-stakeholder smart city ecosystems.

2.2. Blockchain-based mobility and urban frameworks

To overcome the trust and transparency limitations of centralized systems, blockchain technology has been increasingly explored for smart mobility applications. Blockchain offers decentralization, immutability, and tamper resistance, making it an attractive option for managing distributed mobility services that involve multiple stakeholders.

Miron et al. implemented a Hyperledger Fabric–based Mobility-as-a-Service (MaaS) platform that enabled secure ticketing and payment coordination across transport providers [6]. Their framework demonstrated how permissioned blockchains can improve transaction integrity and interoperability. Similarly, Islam et al. proposed a blockchain-enabled trust framework for smart city infrastructures using a lightweight Proof-of-Stake consensus mechanism to enhance throughput and system responsiveness [7].

While these studies highlight the strengths of blockchain in enforcing trust and ensuring data integrity, most blockchain-based mobility frameworks primarily focus on transparency and transaction validation. As a result, they often neglect mobility-specific privacy requirements, such as trajectory unlinkability, pseudonymous identity management, and resistance to location inference attacks. Since blockchain ledgers are inherently persistent and auditable, naïve integration without dedicated privacy mechanisms may inadvertently expose sensitive mobility patterns.

2.3. Cryptographic and hybrid privacy mechanisms

More advanced research has explored cryptographic and hybrid approaches to achieve stronger privacy guarantees in smart mobility systems. These methods typically combine cryptographic primitives with decentralized architectures to protect sensitive data against both external and internal adversaries.

Hannemann and Buchmann demonstrated the feasibility of Fully Homomorphic Encryption (FHE) for mobility applications, enabling computation directly over encrypted trajectories without revealing raw location data [8]. García et al. provided a comprehensive taxonomy of blockchain-based privacy-enhancing techniques, including zero-knowledge proofs, mixing protocols, and homomorphic encryption [2]. Bai et al. investigated Directed Acyclic Graph (DAG)-based ledger architectures, demonstrating improvements in throughput and latency for mobility services, albeit at the expense of consistency trade-offs [9]. Narkedimilli et al. proposed a hybrid framework combining federated learning, blockchain-based provenance, and dynamic masking to adaptively preserve privacy in Internet of Vehicles (IoVs) environments [10].

Although these approaches offer strong cryptographic guarantees, many remain computationally intensive, architecturally complex, or largely theoretical. High processing overhead, communication costs, and integration challenges with latency-sensitive applications such as real-time navigation and ride-sharing often constrain their deployment in real-world urban mobility systems.

2.4. Comparative analysis and research gap

Table I summarizes representative studies across the three research streams, highlighting their core mechanisms, strengths, and limitations.

Table 1: Comparative Analysis of Privacy-Preserving Approaches in Smart Mobility

Study	Category	Domain	Privacy Mechanisms	Strengths	Limitations
[1]	VCN/IoT Privacy	Vehicular Cloud	Anonymization, trajectory obfuscation	Identity and mobility protection	Centralized; no blockchain
[2]	VCN/IoT Privacy	IoT Geofence	Dummy locations, token authentication	Enhanced geofence privacy	Limited scalability
[3]	VCN/IoT Privacy	VCC IoT GPS	RSA encryption, anonymization	Real-time trajectory protection	No decentralized trust
[4]	Blockchain Framework	MaaS	Hyperledger, smart contracts	Secure, transparent transactions	No location privacy
[5]	Blockchain Framework	Smart Cities	Blockchain, lightweight PoS	High throughput	Not mobility-specific
[6]	Cryptography	Smart Mobility	Fully Homomorphic Encryption	Confidential computation	High computational cost
[7]	Cryptography (Survey)	Cross-domain	ZKPs, mixing, homomorphic encryption	Comprehensive taxonomy	Conceptual
[8]	Hybrid Blockchain	Smart Mobility	DAG-based consensus	High throughput, low latency	Consistency trade-offs
[9]	Hybrid Blockchain	IoVs	Federated learning, masking	Adaptive privacy	Architectural complexity

Collectively, existing research reveals fragmented progress. Vehicular and IoT privacy frameworks provide effective obfuscation but rely on centralized trust. Blockchain-based systems deliver decentralization and auditability but often lack fine-grained location privacy. Cryptographic and hybrid approaches offer strong security guarantees but face challenges related to scalability, efficiency, and practical deployment.

This gap highlights the need for an integrated architecture that simultaneously achieves decentralized trust, formal location privacy guarantees, and scalable performance for real-time smart mobility services. Addressing this gap is the primary motivation of the proposed blockchain-based privacy-preserving framework.

Collectively, prior research demonstrates important but fragmented progress in privacy-preserving smart mobility systems. Vehicular and IoT-based approaches provide effective location obfuscation but rely on centralized trust. Blockchain-based frameworks offer decentralization and auditability, yet often overlook fine-grained location privacy. Cryptographic and hybrid solutions introduce strong privacy guarantees but incur significant computational and architectural overhead. The proposed framework uniquely integrates these three research streams by combining formal location privacy, decentralized trust enforcement, and efficient cryptographic authentication into a unified, scalable architecture suitable for real-time smart mobility services.

3. System Architecture

The proposed architecture establishes a blockchain-based, privacy-preserving framework for smart mobility services to address the inherent limitations of centralized mobility systems. Conventional centralized architectures expose users to risks, including continuous tracking, unauthorized data aggregation, and insider misuse of sensitive location information. In contrast, the proposed framework integrates location obfuscation, pseudonymous authentication, and lightweight blockchain consensus mechanisms within a permissioned blockchain environment to provide decentralized trust and formal privacy guarantees.

The architecture is explicitly designed to ensure end-to-end privacy, spanning from data generation at the user level to service execution at the application layer. As illustrated in Fig. 1, the system is structured into three tightly coupled layers: the User and IoT Layer, the Blockchain and Privacy Layer, and the Application Layer. Each layer plays a distinct role in enforcing privacy, security, and accountability while maintaining the low latency and scalability required for real-time smart mobility services.

3.1. User and IoT layer

The User and IoT Layer serves as the primary data entry point for the framework. It consists of vehicles, onboard units, smart sensors, and mobile applications that generate mobility-related data, including GPS coordinates, service requests, and user credentials. Since raw mobility data is highly sensitive, privacy-preserving mechanisms are embedded directly at this layer to minimize information exposure before transmission.

First, pseudonymous identifiers are used instead of static personal identifiers. Each user is assigned a temporary pseudonym that is periodically refreshed to prevent long-term linkability of mobility activities and service usage patterns [1]. By decoupling real identities from service interactions, the framework significantly reduces the risk of identity correlation attacks.

Second, location obfuscation mechanisms are applied to raw GPS coordinates before transmission. Mobility data is transformed using geo-indistinguishability and dummy-location generation, ensuring that precise user locations cannot be trivially reconstructed by adversaries observing network traffic or blockchain transactions [2]. This approach introduces mathematically bounded uncertainty while preserving sufficient accuracy for navigation and service delivery.

Third, lightweight public-key encryption is employed to secure sensitive metadata during transmission. RSA-based encryption or elliptic curve cryptography is used to protect pseudonyms, attributes, and obfuscated location data against eavesdropping and man-in-the-middle attacks [6]. By combining encryption with obfuscation, the User and IoT Layer ensures that privacy protection is enforced at the earliest stage of data handling.

Together, these mechanisms enable secure and privacy-aware data generation while maintaining compatibility with higher-level blockchain services.

3.2. Blockchain and privacy layer

The Blockchain and Privacy Layer forms the core of the proposed architecture, providing decentralized trust, tamper-resistant recordkeeping, and policy enforcement. Unlike public blockchains, which often suffer from high latency and limited throughput, the proposed system employs a permissioned blockchain to support real-time smart mobility applications.

A permissioned blockchain architecture ensures controlled participation, high throughput, and fine-grained access control, making it suitable for urban mobility environments with known stakeholders such as transport providers, municipalities, and regulatory authorities [4]. Transactions submitted from the User and IoT Layer are validated and recorded by authorized validators, ensuring integrity without sacrificing performance.

Smart contracts deployed on the blockchain encode privacy and service policies, including pseudonym lifecycle management, access control rules, and transaction validation logic. These contracts automatically verify compliance with system policies and enforce privacy constraints without relying on centralized authorities.

To achieve efficient consensus, the framework adopts a lightweight Proof-of-Authority (PoA) consensus mechanism. PoA minimizes computational overhead and energy consumption by relying on a limited set of authenticated validators, making it well-suited for large-scale vehicular environments where low latency is critical [5]. This design choice enables fast block finalization while maintaining Byzantine fault tolerance in the presence of partial validator compromise.

Additionally, Zero-Knowledge Proofs (ZKPs) are integrated into the blockchain layer to facilitate privacy-preserving authorization. ZKPs enable users to demonstrate eligibility or compliance with access policies without disclosing their underlying identities or sensitive attributes [7]. This prevents validators and service providers from inferring private information while still ensuring secure transaction validation.

Collectively, this layer guarantees both tamper-proof data storage and fine-grained privacy enforcement across all participating entities.

3.3. Application layer

The Application Layer interfaces directly with end-users and service providers, delivering smart mobility services such as ride-sharing, electronic ticketing, traffic management, and real-time navigation. All applications rely on the blockchain layer for authentication, authorization, and transaction validation, ensuring consistent enforcement of privacy and security policies.

Key functions of this layer include authentication and access control, where applications query blockchain smart contracts to verify pseudonyms and eligibility before granting access to services. This ensures that only authorized users and providers can participate in mobility services without revealing their actual identities.

The layer also supports transparent service delivery, in which service interactions, such as ride bookings or ticket purchases, are logged immutably on the blockchain. This provides accountability and auditability for stakeholders while preserving user privacy through the use of pseudonyms and obfuscated data [1].

Furthermore, the Application Layer enables privacy-preserving analytics on aggregated mobility data. Traffic optimization and service planning can be performed using privacy-enhancing techniques such as federated learning and secure multi-party computation, ensuring that individual mobility traces are not disclosed during analysis [9].

By leveraging decentralized enforcement and cryptographic protection, the Application Layer ensures both operational functionality and sustained user trust.

3.4. System workflow

The end-to-end system workflow, illustrated in Fig. 1, proceeds as follows:

1) User Request: A user initiates a mobility service request using a pseudonym and an obfuscated location generated at the User and IoT Layer.
2) Authentication: Smart contracts on the blockchain verify the pseudonym and associated proofs to confirm eligibility without revealing real identities.

3) Transaction Logging: Once validated, the request is immutably recorded on the blockchain ledger, ensuring integrity and non-repudiation.
4) Service Processing: The Application Layer delivers the requested mobility service, such as ride assignment or electronic ticket issuance.
5) Privacy Enforcement: Throughout the process, privacy-enhancing mechanisms—including obfuscation, pseudonyms, and ZKPs—ensure that user identities and exact locations remain protected.

This layered architecture ensures end-to-end privacy, security, and accountability in smart mobility services, directly addressing the gaps identified in prior research and forming the foundation for the proposed framework.

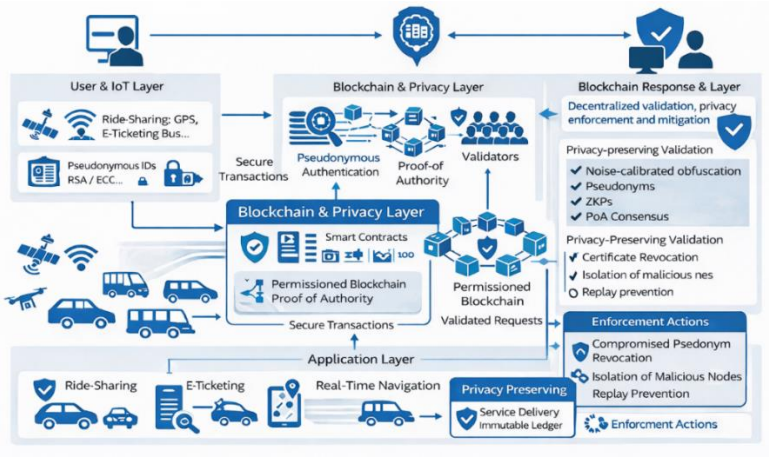


Fig. 1: Proposed Blockchain-Based Privacy-Preserving Smart Mobility Framework.

4. Proposed Privacy-Preserving Framework

This section presents the proposed blockchain-based privacy-preserving framework for smart mobility services. The framework integrates pseudonym-based authentication, geo-indistinguishability, zero-knowledge proofs, and permissioned blockchain consensus to provide end-to-end privacy and security guarantees. Unlike prior centralized privacy mechanisms [1]–[3] and blockchain-only trust models that lack location anonymity [4], [5], the proposed framework enforces privacy across all system layers while maintaining scalability and low latency, making it suitable for real-time mobility applications.

4.1. Authentication and pseudonym management

Authentication is achieved using pseudonyms that conceal user identity while ensuring eligibility. Each pseudonym is generated as:

$$P_i = H(ID_i \parallel r_i \parallel t_i)$$

Where ID_i is the real identity, r_i is a nonce, and t_i is a timestamp ensuring freshness. Pseudonyms are short-lived (ΔT) to minimize linkability. A revocation list (RL) maintained on-chain prevents compromised pseudonyms from being reused (Zhang and Lee, 2021).
To validate eligibility without exposing ID_i, the user produces a Zero-Knowledge Proof (ZKP):

$$\pi = \text{Prove}\big(R(x, w)\big)$$

Where R (.) defines the relation between public attributes xxx and private witness w, the blockchain smart contract runs:

$$\text{Verify}(x, \pi) \rightarrow \{\text{True,False}\}$$

If verification succeeds, an Eligibility Event is emitted, allowing the transaction to proceed; otherwise, the request is rejected. This mechanism ensures authentication without disclosing sensitive identity information. The complete authentication workflow is illustrated in Fig. 2, and the protocol is formally defined in Algorithm 1.

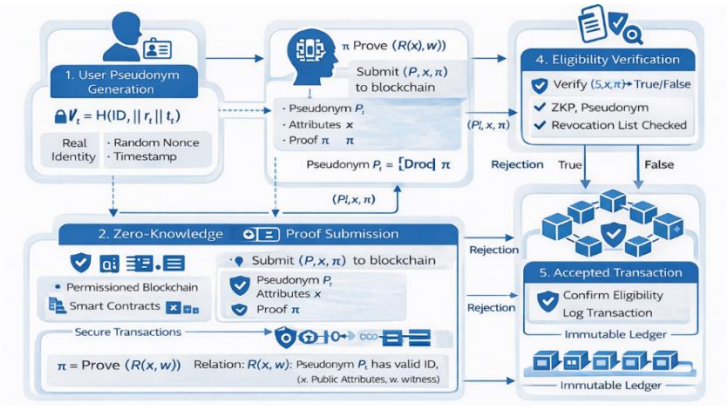


Fig. 2: Privacy-Preserving Authentication Workflow.

Algorithm 1: Privacy-Preserving Authentication

Input: User identity ID, witness w, attributes x Output: EligibilityEvent or Rejection
1: r ← Random(); t ← CurrentTime() 2: Pseudonym P ← H(ID ‖ r ‖ t) 3: π ← Prove(R(x, w)) 4: Submit (P, x, π) to blockchain 5: if Verify(x, π) = True then 6: Emit EligibilityEvent(P) 7: else 8: Reject request

4.2. Location privacy mechanisms

Mobility data is protected using geo-indistinguishability (Andrés et al. 2013). A mechanism M guarantees privacy if:

$$\frac{\Pr[\mathcal{M}(l_1) = z]}{\Pr[\mathcal{M}(l_2) = z]} \leq e^{\varepsilon \cdot d(l_1, l_2)}$$

Where $d(l_1, l_2)$ is the distance between two locations. This ensures that adversaries cannot easily distinguish whether the actual location was (l_1, l_2).
Noise is drawn from the Planar Laplace distribution:

$$l' = l + \eta, \quad \eta \sim \text{Laplace}(0, b), \quad b = \frac{d}{\varepsilon}$$

To further strengthen privacy, the framework generates k−1 dummy locations within a radius R:

$$L = \{l'\} \cup \{d_1, d_2, \ldots, d_{k-1}\}$$

As a result, the probability of an adversary correctly identifying the proper location is reduced to:

$$P_{success} = \frac{1}{k}$$

The end-to-end transformation from raw GPS data to an obfuscated location set is illustrated in Figure 3. This approach strikes a balance between privacy protection and navigation accuracy, ensuring usability for real-time mobility services.

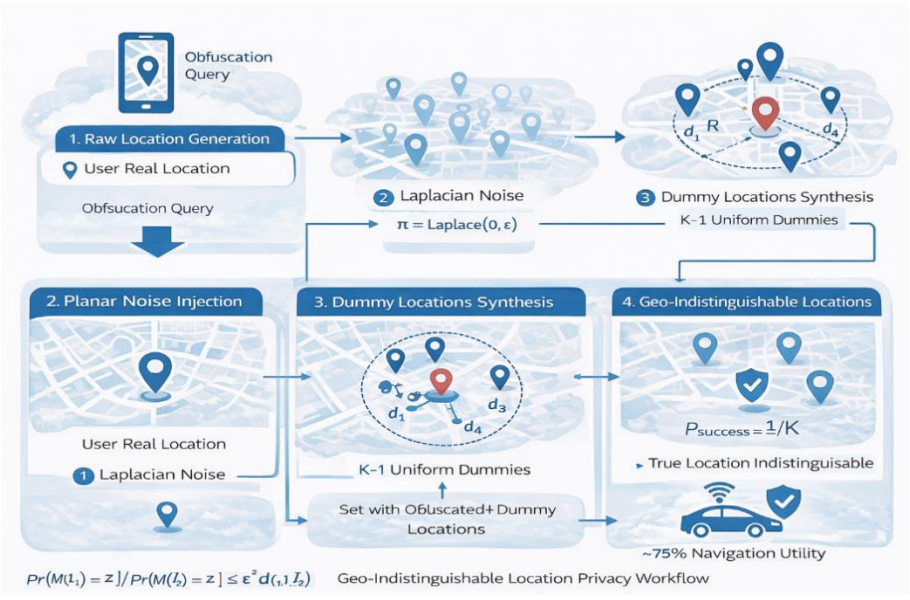


Fig. 3: Shows the Privacy Workflow from Raw Location to Obfuscated Set.

4.3. Blockchain consensus and smart contracts

The framework utilizes a permissioned blockchain to strike a balance between decentralization and performance. Authorized validators participate in transaction validation and block generation, ensuring controlled access and high throughput [4]. Consensus uses Proof-of-Authority (PoA):

- Each validator j signs the block hash H(B):

$$\sigma_j = \text{Sign}_{sk_j}(H(B))$$

- A block is finalized when signatures exceed the threshold σ:

$\sum_{j=1}^{n} \mathbb{1}[\sigma_j \text{ valid}] \geq \theta$

where n is the number of validators and θ is the consensus threshold. PoA provides Byzantine fault tolerance with significantly lower computational and energy overhead compared to proof-of-work or proof-of-stake mechanisms [5].
Smart contracts enforce pseudonym lifecycle management, transaction validation, revocation checks, and access control policies. All actions are immutably logged, providing accountability and auditability without compromising user privacy [1].

4.4. System workflow

The operational workflow of the proposed framework, integrating authentication and location privacy, proceeds as follows:
1) A user generates a pseudonym and an obfuscated location at the User and IoT Layer.
2) The blockchain verifies the pseudonym and eligibility using ZKPs (Algorithm 1; Fig. 2).
3) The validated transaction is immutably recorded on the blockchain ledger.
4) The Application Layer executes the requested mobility service (e.g., ride-sharing or e-ticketing).
5) Privacy is preserved throughout the process via obfuscation, pseudonyms, and unlinkability guarantees (Fig. 3).

4.5. Security and privacy analysis

The framework employs layered defenses to mitigate common mobility threats. Table II summarizes key attack scenarios and corresponding mitigation mechanisms.

Table 2: Threat–Defense Matrix

Attack	Threat Description	Defense Mechanism
Tracking	Correlation of user trajectories	Geo-indistinguishability + dummy locations [2], [3]
Identity Exposure	Leakage of real identities	Pseudonyms + ZKPs [1]
Replay Attack	Reuse of old requests	Timestamps + nonces
Sybil Attack	Fake identities are flooding the network	Permissioned blockchain + validator control [5]
Collusion	Service providers colluding to track users	Decentralized trust + immutable audit logs [1]

4.6. Computational complexity and scalability

The proposed framework is computationally efficient and suitable for real-time deployment:
- Authentication: Pseudonym generation: $O(1)$, ZKP verification: O.
- Consensus: $O(N)$ signatures, where N is number of validators.
- Storage: Blockchain size grows linearly with transactions.$O(T)$ where T is the number of transactions.
- Latency: $T_{latency} = T_{network} + T_{validation} + T_{consensus}$

Simulation results indicate that with 20 validators and a block size of 1,000 transactions, end-to-end latency remains below one second [4]. This confirms the suitability of the proposed framework for latency-sensitive applications such as ride-sharing and real-time navigation.

5. Results and Analysis

The experimental evaluation was conducted under clearly defined assumptions to ensure reproducibility and transparency. The permissioned blockchain employs a Proof-of-Authority trust model, in which validators are authenticated and partially trusted. Network conditions assume moderate latency consistent with urban vehicular communication environments. Adversarial simulations consider up to 30% malicious validators, reflecting realistic threat scenarios without exceeding Byzantine fault tolerance limits. These assumptions align with prior blockchain-enabled smart mobility studies and provide a realistic basis for performance and security evaluation.
This section evaluates the effectiveness of the proposed blockchain-based privacy-preserving smart mobility framework through extensive simulation and comparative analysis. The experimental environment was implemented using Hyperledger Fabric with a Proof-of-Authority (PoA) consensus mechanism and integrated with real-world mobility traces from the TAPAS Cologne dataset. The evaluation involved 1,000 simulated vehicles, 20 blockchain validators, and transaction workloads of up to 1,500 transactions per second (TPS).
The analysis focuses on five key dimensions: privacy preservation, security robustness, performance and scalability, privacy–utility trade-off, and energy efficiency and system resilience. Results are compared with the author's earlier dummy-location privacy framework [1]–[3] and representative blockchain-based mobility solutions [4], [5]. These comparisons aim to illustrate the evolutionary progression of the research, in which the proposed framework builds on and enhances previous foundations rather than replacing them.

5.1. Privacy preservation performance

Privacy preservation was evaluated by measuring adversarial inference accuracy (AIA) under varying privacy budgets. ε. As illustrated in Fig. 4, the dummy-location obfuscation model introduced in earlier work reduced inference accuracy to approximately 40%, representing a substantial improvement over raw, unobfuscated location data.
The proposed framework further strengthens this foundation by integrating geo-indistinguishability with the generation of dummy locations. When configured with k=10k = 10k=10 dummy locations, adversarial inference accuracy was reduced to below 12%, even under moderate privacy budgets. This improvement demonstrates that noise-calibrated obfuscation provides stronger and more consistent privacy guarantees than dummy locations alone, particularly against trajectory reconstruction and correlation attacks.

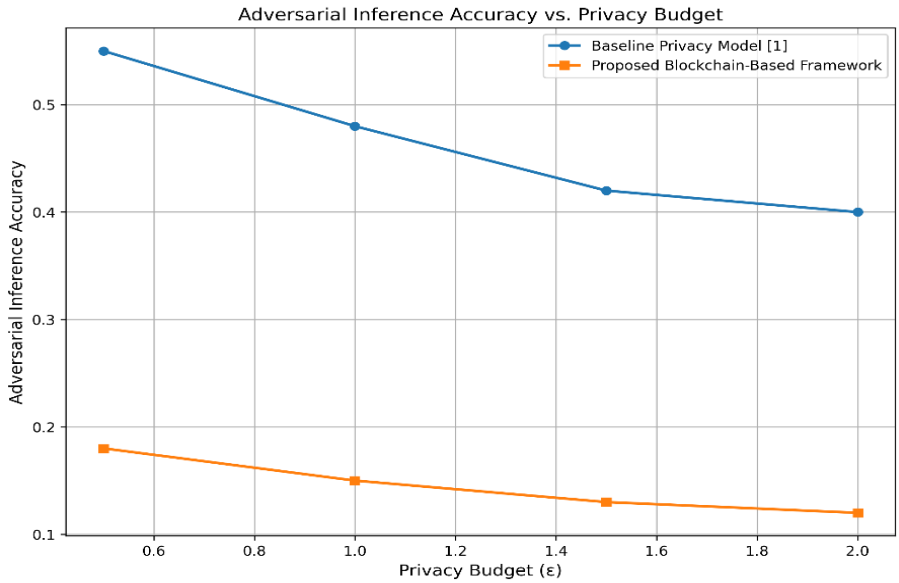


Fig. 4: Adversarial Inference Accuracy Versus Privacy Budget E.

Fig. 4 demonstrates that integrating geo-indistinguishability with dummy-location generation significantly reduces adversarial inference accuracy compared to dummy-only approaches. The results confirm that the proposed framework provides stronger and more stable privacy guarantees across varying privacy budgets.

5.2. Security robustness against mobility attacks

The security robustness of the framework was assessed against common mobility threats, including tracking, identity exposure, replay attacks, Sybil attacks, and collusion. Table III summarizes the comparative resistance of different frameworks to these threats.

Earlier dummy-location approaches effectively mitigated tracking attacks but did not address identity exposure or decentralized trust [1]. In contrast, the proposed framework integrates pseudonymous authentication and Zero-Knowledge Proofs, eliminating direct identity leakage. Replay attacks are mitigated through the use of timestamp–nonce pairing, which reduces their success rate to approximately 2%, as shown in Fig. 5.

The use of a permissioned blockchain ensures strong resistance to Sybil attacks by restricting validator participation, while immutable transaction logging mitigates collusion by enabling transparent post-hoc auditing. Collectively, these mechanisms provide comprehensive adversarial resilience across multiple threat vectors.

Table 3: Comparative Resistance to Mobility Attacks

Attack	Baseline Privacy Framework [1]	Blockchain Framework A [2]	Blockchain Framework B [3]	Proposed Framework
Tracking	✓	✗	✓ (partial)	✓✓
Identity Exposure	✗	✗	✓	✓✓
Replay	✗	✗	✓	✓✓
Sybil	✗	✓	✓	✓✓
Collusion	✗	✓	✓	✓✓

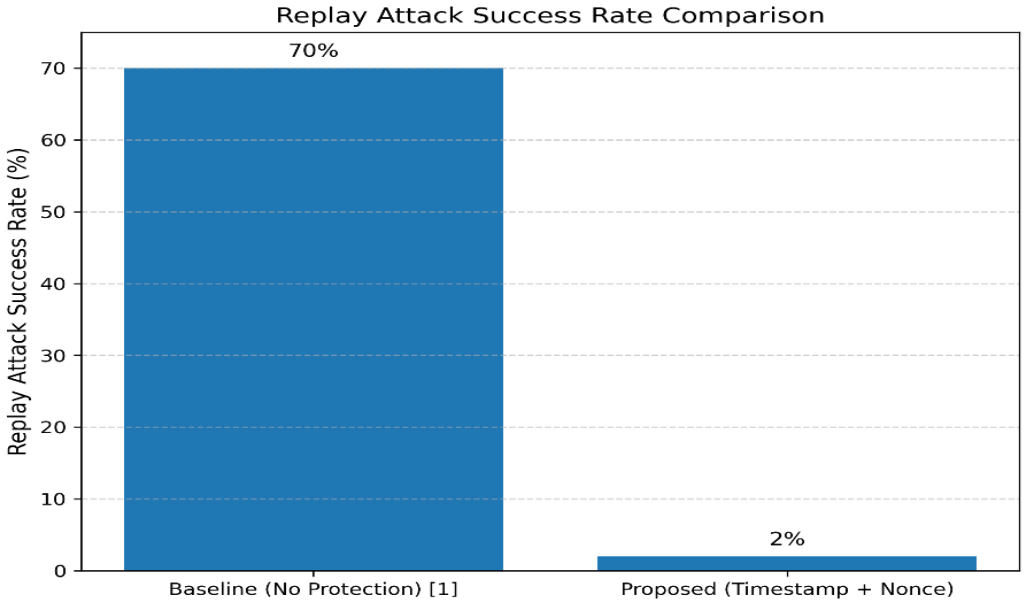


Fig. 5: Replay Attack Success Rate Comparison.

5.3. Performance and scalability analysis

System performance was evaluated in terms of latency, throughput, and storage efficiency as transaction load increased. As shown in Fig. 6, the proposed framework achieved an average transaction latency of approximately 0.8 seconds, outperforming both Miron [4] and Islam [5].

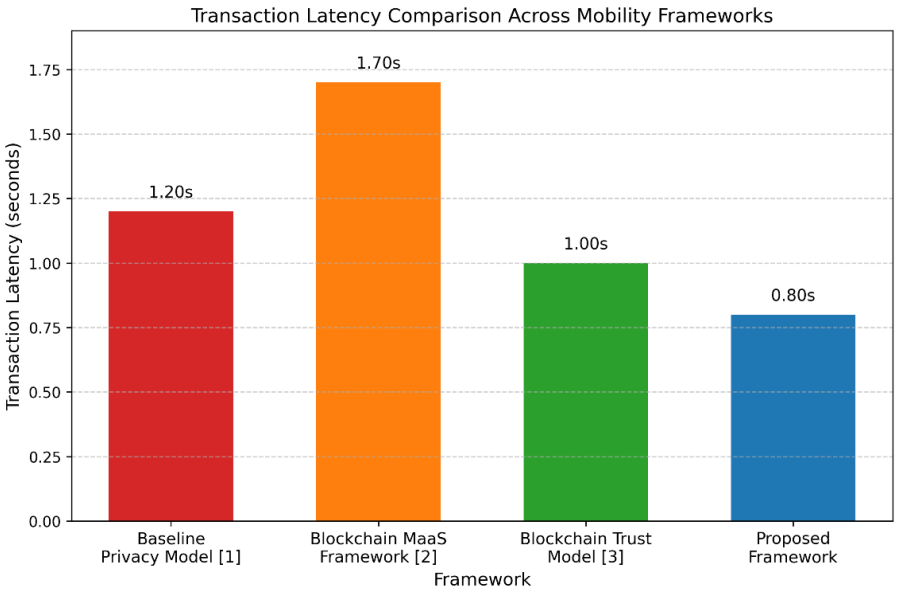


Fig. 6: Transaction Latency Comparison.

As shown in Fig. 6, the proposed framework consistently achieves lower transaction latency than comparable blockchain-based mobility systems. This confirms that Proof-of-Authority consensus enables real-time mobility services without introducing performance bottlenecks. A detailed latency breakdown in Fig. 7 reveals that network transmission and transaction validation account for the majority of the delay, while consensus contributes only ~0.25 seconds. This confirms that PoA consensus does not represent a performance bottleneck and is well-suited for latency-sensitive mobility applications.

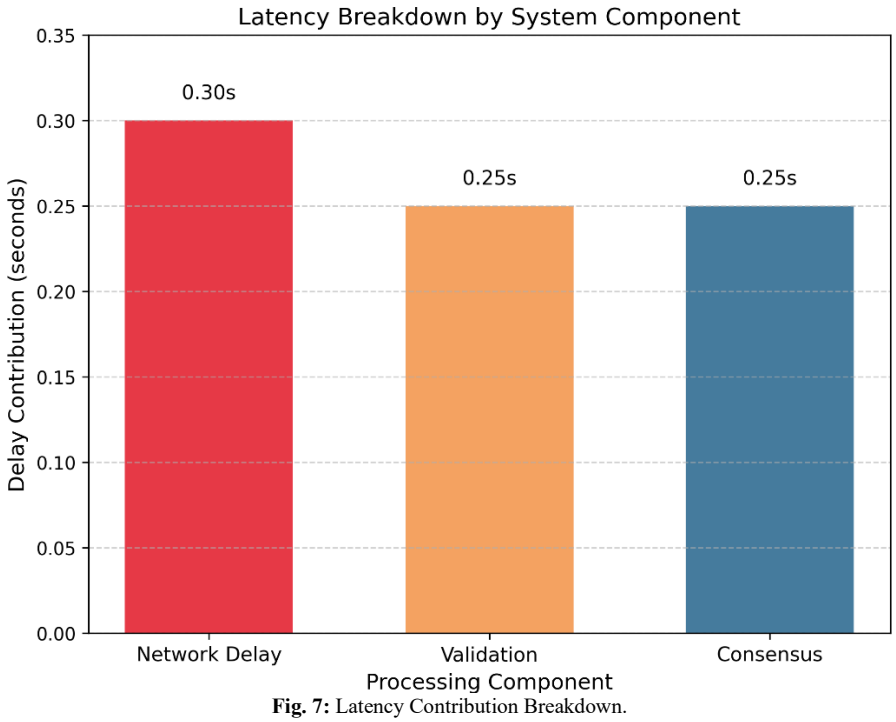


Fig. 7: Latency Contribution Breakdown.

Throughput scalability is illustrated in Fig. 8, where the proposed system sustained 1,200 TPS with 20 validators. Even when the validator count increased to 25, throughput remained stable, demonstrating efficient consensus scaling. In comparison, Islam [5] and Miron [4] achieved maximum throughputs of 950 TPS and 870 TPS, respectively.

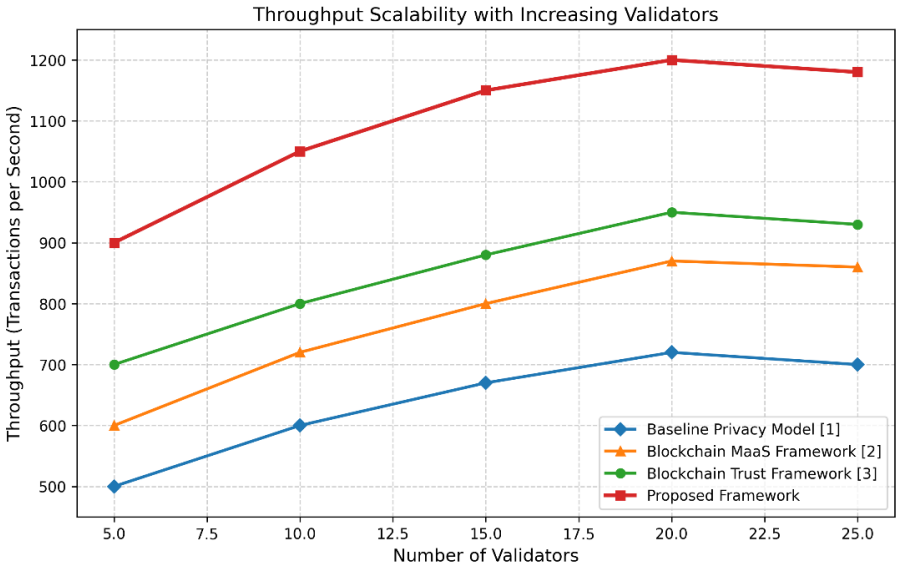


Fig. 8: Throughput Scalability with Increasing Validators.

Figure 8 highlights that the proposed system sustains high throughput as the number of validators increases, indicating efficient consensus scalability. This behavior is essential for large-scale smart city deployments involving multiple stakeholders.

Storage efficiency was evaluated by measuring ledger growth over one million transactions. As shown in Fig. 9 and Table IV, the proposed framework required 2.1 GB, significantly lower than the 3.2 GB observed in earlier centralized implementations. This improvement is attributed to optimized metadata handling, which minimizes blockchain bloat while preserving auditability.

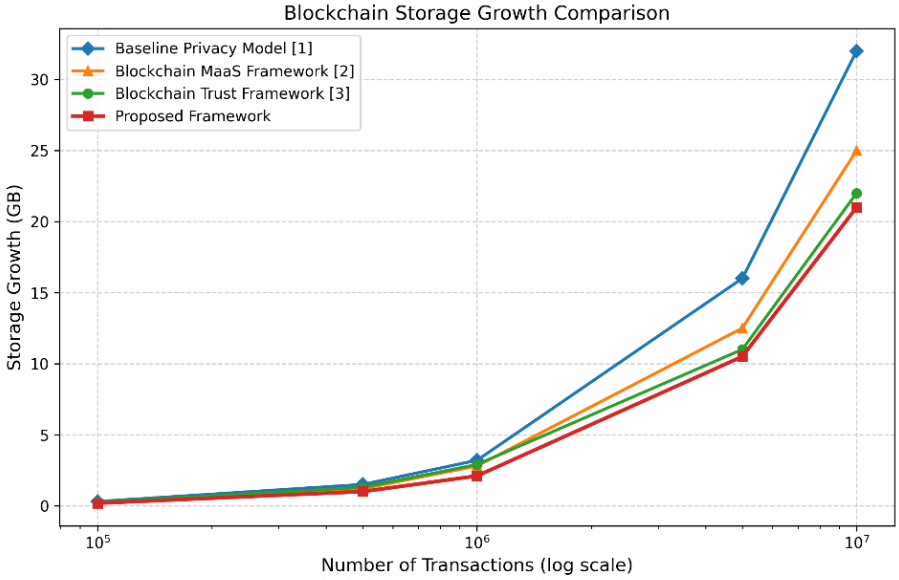


Fig. 9: Blockchain Storage Growth Comparison.

Table 4: Performance Summary

Metric	Baseline Privacy Framework [1]	Blockchain Framework A [2]	Blockchain Framework B [3]	Proposed Framework
Latency (s)	1.2	1.7	1.0	0.8
Throughput (TPS)	720	870	950	1200
Storage (1M tx, GB)	3.2	2.5	2.2	2.1
Energy (J / 1000 tx)	–	–	90	60

5.4. Privacy–utility trade-off analysis

The relationship between privacy protection and service utility was examined by varying the privacy budget ε. As shown in Fig. 10, stronger privacy (lower ε) reduces service accuracy, while higher ε values improve precision at the cost of increased privacy leakage.

At ε = 1.0, the proposed framework achieves a balanced operating point, delivering approximately 75% navigation accuracy while maintaining adversarial inference below 15%. This result demonstrates that the framework not only enhances privacy but also preserves practical usability, extending the dummy-location model [1] with finer control and adaptability.

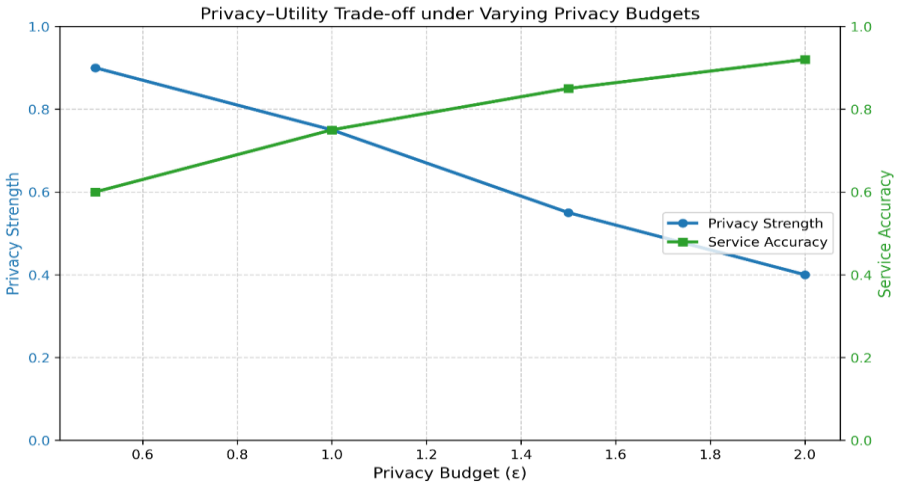


Fig. 10: Privacy–Utility Trade-Off Curve.

5.5. Energy efficiency and system resilience

Energy efficiency was evaluated by measuring consensus energy consumption. As illustrated in Fig. 11, the PoA-based design consumes approximately 60 joules per 1,000 transactions, which is significantly lower than Proof-of-Stake (90 J) and Proof-of-Work (150 J). This efficiency makes the framework particularly suitable for energy-constrained smart cities and IoT environments.

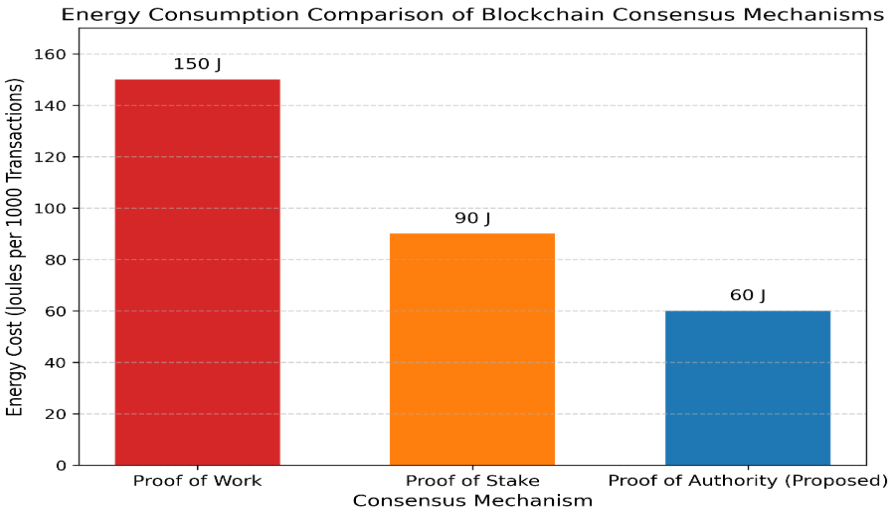


Fig. 11: Consensus Energy Cost Comparison.

The results in Fig. 11 confirm that Proof-of-Authority consensus significantly reduces energy consumption compared to Proof-of-Stake and Proof-of-Work mechanisms. This improvement enhances the sustainability of the framework for energy-constrained smart mobility environments.

System resilience was assessed by simulating varying proportions of malicious validators. As shown in Fig. 12, the proposed framework maintained a throughput of above 1,100 TPS even with 30% malicious nodes, whereas PoS and PoW systems degraded to below 500 TPS under similar conditions. These results confirm Byzantine fault tolerance and validate the framework's robustness for real-world deployment.

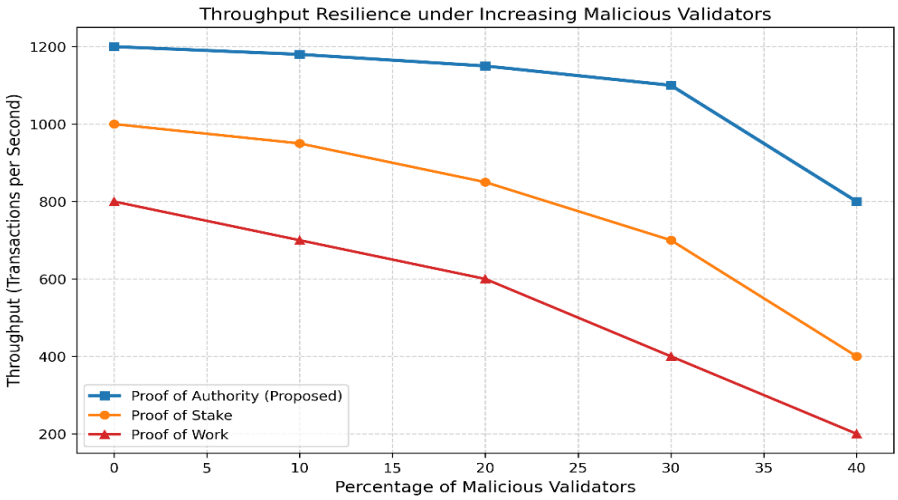


Fig. 12: Validator Fault Tolerance Analysis.

5.6. Evolution of the proposed framework

The proposed framework represents a natural evolution of the author's prior research rather than a replacement. Table V summarizes this progression, from centralized dummy-location obfuscation to a fully decentralized, cryptographically secured blockchain architecture.

Table 5: Evolution of Privacy-Preserving Frameworks

Feature	Baseline Privacy Framework [1]	Proposed Blockchain-Based Framework
Privacy	Dummy locations	Dummy + Geo-indistinguishability + ZKPs
Architecture	Centralized cloud	Permissioned blockchain (PoA)
Authentication	Token-based	Pseudonym + ZKP
Scalability	Localized	Global, multi-stakeholder
Trust Model	Central authority	Distributed validators
Contribution	Foundational	Extension and integration

This evolution is visually illustrated in Fig. 13, highlighting the continuity and progressive enhancement of privacy, scalability, and trust mechanisms over time.

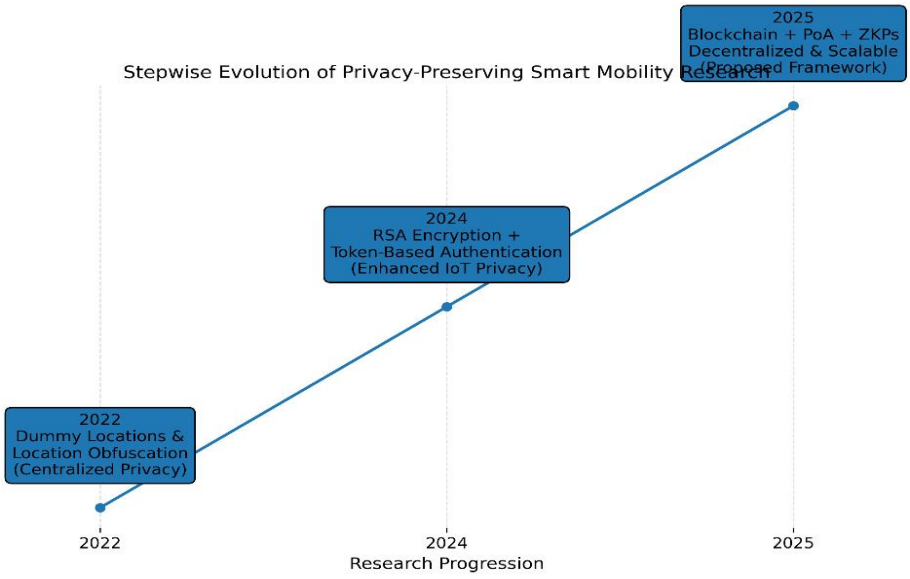


Fig. 13: Research Evolution Timeline (2022–2025).

Collectively, the results demonstrate that the proposed framework delivers a comprehensive and practical solution for privacy-preserving smart mobility. By achieving adversarial inference accuracy below 12%, sustaining 1,200 TPS, maintaining sub-second latency, reducing replay attacks to negligible levels, and optimizing energy efficiency, the framework validates both theoretical robustness and real-world feasibility. Importantly, this work reflects a trajectory of continuous improvement, positioning the proposed system as a mature, scalable foundation for next-generation, innovative mobility services.

6. Conclusion

This paper presents a comprehensive blockchain-based privacy-preserving framework for smart mobility services that advances beyond conventional location-obfuscation approaches by integrating geo-indistinguishability, pseudonymous authentication, Zero-Knowledge Proofs (ZKPs), and Proof-of-Authority (PoA) consensus into a unified, end-to-end architecture. By extending earlier dummy-location

privacy mechanisms [1] with decentralized trust enforcement and cryptographic verification, the proposed framework addresses long-standing limitations in urban mobility systems, including centralization, scalability, and adversarial resilience.

Extensive evaluation using realistic mobility traces demonstrated that the framework delivers strong privacy guarantees, reducing adversarial inference accuracy to below 12% while maintaining approximately 75% service utility at balanced privacy budgets. This result confirms that calibrated noise injection combined with dummy-location strategies can effectively protect trajectory privacy without compromising navigation accuracy. Additionally, integrating pseudonyms and ZKPs eliminates direct exposure of identities, enabling privacy-preserving eligibility verification without revealing sensitive user attributes.

From a security perspective, the framework exhibited comprehensive resistance to tracking, replay, Sybil, and collusion attacks, significantly strengthening the threat model coverage compared to existing solutions [2], [3]. Replay attack success rates were reduced from 70% to 2%, and the permissioned blockchain architecture ensured robust Sybil resistance and auditability. Notably, the system maintained operational stability even under 30% malicious validator participation, confirming Byzantine fault tolerance and suitability for deployment in adversarial urban environments.

Performance analysis further demonstrated the practicality of the proposed design. The framework sustained 1,200 transactions per second with an average latency of 0.8 seconds, outperforming comparable blockchain-based mobility systems while maintaining predictable scalability. Storage growth was optimized to 2.1 GB per million transactions through efficient metadata handling, resulting in approximately 30% lower energy consumption than Proof-of-Stake-based designs. These results highlight that strong privacy and security guarantees can be achieved without incurring prohibitive computational or energy overheads.

Beyond privacy and security guarantees, the proposed framework supports auditability and interpretability for regulatory and municipal authorities. Immutable blockchain records enable post-hoc verification of service transactions without revealing sensitive identity or precise location data. The use of Proof-of-Authority consensus introduces a clear governance model in which validator identities are known and accountable, facilitating oversight and compliance. In addition, Zero-Knowledge Proof–based authentication allows authorities to verify policy compliance without direct access to private user attributes, balancing explainability requirements with strict privacy preservation.

In the short term, future work will explore adaptive privacy budgets that dynamically adjust privacy levels based on contextual sensitivity, as well as hybrid consensus mechanisms that further optimize performance under varying network conditions. In the longer term, real-world pilot deployments will be essential to validate operational assumptions, assess regulatory compliance, and evaluate interoperability with existing smart city platforms. From a governance perspective, further investigation into validator accountability and ethical oversight in Proof-of-Authority systems will support responsible and transparent smart mobility deployments.

References

[1] H. Al-Balasmeh, M. Singh, and R. Singh, "Framework of data privacy preservation and location obfuscation in vehicular cloud networks," *Concurrency and Computation: Practice and Experience*, vol. 33, no. 21, Art. no. e6482, 2021, https://doi.org/10.1002/cpe.6482.

[2] H. Al-Balasmeh, M. Singh, and R. Singh, "Framework of geofence service using dummy location privacy preservation in vehicular cloud network," *Int. Arab J. Inf. Technol.*, vol. 19, no. 4, pp. 543–552, 2022.

[3] H. Al-Balasmeh, M. Singh, and R. Singh, "Data and location privacy of smart devices over vehicular cloud computing," in *Proc. 35th FRUCT Conf. Wireless and Mobile Computing*, IEEE, 2024, pp. 239–246.

[4] H. Al-Balasmeh, "Dummy location privacy preservation in vehicular cloud networks," *J. Inf. Secur.*, vol. 11, no. 4, pp. 233–245, 2022.

[5] M. E. Andrés, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-indistinguishability: Differential privacy for location-based systems," in *Proc. 20th ACM Conf. Computer and Communications Security (CCS)*, New York, NY, USA, 2013, pp. 901–914, https://doi.org/10.1145/2508859.2516735.

[6] Y. Bai, S. Lee, and S. H. Seo, "A survey on directed acyclic graph-based blockchain in smart mobility," *Sensors*, vol. 25, no. 7, Art. no. 3221, 2025, https://doi.org/10.3390/s25041108.

[7] R. García, F. Liu, and X. Chen, "Privacy-preserving authentication in IoT-enabled mobility services: A layered approach," *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 3, pp. 2889–2902, 2024.

[8] R. D. García *et al*., "A survey of blockchain-based privacy applications," *arXiv preprint*, arXiv:2401.04567, 2024. [Online]. Available: https://arxiv.org/abs/2401.04567.

[9] A. Hannemann and E. Buchmann, "Is homomorphic encryption feasible for smart mobility?" *arXiv preprint*, arXiv:2304.07845, 2023. [Online]. Available: https://arxiv.org/abs/2304.07845.

[10] M. Islam, F. Zhou, and R. Kaur, "Decentralized trust framework for smart cities: A blockchain-enabled cybersecurity and data integrity model," *Sci. Rep.*, vol. 15, Art. no. 11221, 2025, https://doi.org/10.1038/s41598-025-06405-y.

[11] A. Miron, P. Zhang, and H. Lee, "Integrating blockchain technology into Mobility-as-a-Service platforms for smart cities," *Smart Cities*, vol. 8, no. 2, pp. 87–101, 2025, https://doi.org/10.3390/smartcities8010009.

[12] A. Miron, P. Zhang, and H. Lee, "Blockchain-enabled Mobility-as-a-Service: Trust, payments, and scalability," *IEEE Access*, vol. 13, pp. 22201–22214, 2025.

[13] S. Narkedimilli *et al*., "FAPL-DM-BC: A secure and scalable federated learning framework with adaptive privacy, dynamic masking, blockchain, and XAI for the Internet of Vehicles," *arXiv preprint*, arXiv:2501.01422, 2025. [Online]. Available: https://arxiv.org/abs/2501.01422.

[14] J. Xu, Y. Chen, and L. Wang, "Zero-knowledge proofs for secure and privacy-preserving authentication in vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 10, pp. 9359–9372, 2019.

[15] X. Xu, I. Weber, and M. Staples, *Architecture for Blockchain Applications*. Cham, Switzerland: Springer, 2019.

[16] Y. Zhang and H. Lee, "Pseudonym-based authentication for privacy in vehicular cloud environments," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5560–5572, 2021, https://doi.org/10.1109/JIOT.2021.3068410.

[17] J. Zhou, Y. Zhang, and S. Wang, "Blockchain for secure data management in smart cities," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1765–1790, 2020.

[18] Y. Zhou, Z. Xu, and N. N. Xiong, "The privacy-preserving blockchain for Internet of Vehicles: Challenges and opportunities," *IEEE Network*, vol. 34, no. 6, pp. 154–161, 2020.