Authentication mechanisms in Intelligent Transportation Systems (ITS) are essential to verify the legitimacy of vehicles interacting with roadside infrastructure. Conventional methods, such as static credentials or public key infrastructure (PKI), often fall short in protecting sensitive information. They either expose critical data or suffer from scalability issues, especially in high-density traffic scenarios. Furthermore, these methods may not effectively address emerging security threats, such as replay attacks or data breaches.

Zero-Knowledge Proofs (ZKPs) and One-Time Passwords (OTPs) offer a promising solution to these challenges.

We introduce a novel authentication mechanism for Vehicle-to-Infrastructure (V2I) communication, leveraging ZKPs and OTPs. The proposed framework ensures that vehicles can securely authenticate with infrastructure nodes without exposing sensitive information, such as permanent identities or private keys. By incorporating blockchain technology, the framework also achieves tamper-proof logging of authentication events, further strengthening system integrity.

To evaluate the framework, we conduct extensive simulations using SUMO (Simulation of Urban Mobility) and Mininet, examining its performance, scalability, and security under various traffic scenarios. The results demonstrate the feasibility of deploying ZKP-OTP-based authentication in ITS, highlighting its potential to support large-scale, privacy-preserving communication.

The core of the framework relies on the synergistic integration of ZKPs and OTPs.
Zero-Knowledge Proofs (ZKPs): ZKPs allow a vehicle to prove knowledge of a credential (e.g., a secret key or identity) without revealing the credential itself. This ensures that no sensitive information is leaked during the authentication process. The proposed framework employs zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) to achieve lightweight and efficient proof generation and verification, suitable for the resource-constrained nature of ITS devices. One-Time Passwords (OTPs): OTPs are generated dynamically for each authentication session, ensuring that credentials cannot be reused or intercepted for replay attacks. OTPs are derived using a cryptographic hash function seeded with a shared secret and a timestamp, ensuring their uniqueness and time sensitivity.

ZKP-OTP Authentication Workflow:

Step 1: The vehicle generates an OTP using its unique secret and timestamp.

Step 2: The OTP is embedded into a ZKP, proving that the OTP is valid without revealing the underlying secret or timestamp.

Step 3: The proof is sent to the roadside infrastructure, where the ZKP is verified.

Step 4: Upon successful verification, the vehicle is authenticated, and the session proceeds.

To provide tamper-proof logging and enable decentralized authentication management, the framework integrates blockchain technology. Decentralized Logging: Authentication events, including vehicle identities (anonymized via ZKPs) and session details, are logged onto the blockchain. The immutability of blockchain ensures that these records cannot be altered, providing a reliable audit trail for compliance and dispute resolution. Smart Contract Automation: Smart contracts on the blockchain facilitate real-time verification of ZKPs and OTPs. These contracts are triggered automatically when authentication requests are submitted. The contracts validate the authenticity of proofs and log successful or failed authentication attempts. Dynamic Identity Management: The blockchain maintains a record of temporary identities generated for each session, ensuring privacy while enabling traceability for regulatory compliance when required.

Blockchain Workflow:

Step 1: The ZKP-OTP proof is submitted to the roadside infrastructure.

Step 2: The roadside infrastructure invokes a smart contract on the blockchain, which verifies the proof.

Step 3: The blockchain logs the event, including an anonymized record of the vehicle's identity and authentication status.

Step 4: The outcome is returned to the infrastructure, which grants or denies access.

Privacy Preservation: By combining ZKPs and OTPs, the framework ensures that no sensitive information is exposed during authentication, protecting the vehicle's identity and session details. The use of blockchain further enhances privacy by anonymizing authentication records.

Scalability: Lightweight zk-SNARKs ensure low computational overhead, enabling real-time verification even in high-density traffic scenarios. Blockchain's distributed nature eliminates the need for a centralized authentication server, reducing bottlenecks and increasing fault tolerance.

Resilience to Attacks: Replay attacks are mitigated through the use of OTPs. Man-in-the-middle and tampering attacks are prevented by leveraging the cryptographic guarantees of ZKPs and blockchain immutability. This proposed framework combines the strengths of ZKPs, OTPs, and blockchain to create a robust and efficient authentication system tailored for the dynamic and security-critical environment of ITS. By addressing both privacy and performance requirements, it provides a scalable and future-proof solution for V2I communication.

The experimental setup for evaluating the proposed ZKP-OTP-based authentication framework focuses on simulating real-world vehicle-to-infrastructure (V2I) communication scenarios, measuring performance, privacy, and scalability. The setup integrates multiple tools and

environments, including SUMO (Simulation of Urban Mobility), Mininet, and Ganache, to replicate the dynamic and resource-constrained nature of Intelligent Transportation Systems (ITS).

We employed SUMO (Simulation of Urban Mobility) for simulating vehicular traffic and generating realistic V2I communication scenarios. Routes and road networks are configured to model urban traffic, with vehicles interacting dynamically with roadside infrastructure for authentication. The Mininet network emulator is employed to simulate roadside infrastructure and vehicle communication networks. Infrastructure nodes represent roadside units (RSUs), while host devices simulate vehicular network connectivity. Ganache implements a personal Ethereum blockchain, used to manage authentication events via smart contracts. The blockchain stores authentication logs, proof verifications, and vehicle session data. ZoKrates is a toolkit for generating and verifying zero knowledge proofs (ZKPs). Here, zk-SNARKs are employed to generate lightweight proofs for OTP validation. Custom Python Scripts were developed to integrate these tools, orchestrate simulations, and collect metrics for analysis.

Traffic Simulation: A synthetic urban network with multiple routes and intersections is designed using SUMO. A typical scenario involves 100 vehicles interacting with 10 RSUs, with vehicle densities varied to simulate light, medium, and heavy traffic conditions. Routes are configured in the routes.rou.xml file, and interactions are logged using Python's TraCI API. Authentication Workflows: Each vehicle generates an OTP and submits a ZKP to the nearest RSU. RSUs validate the proof by invoking a smart contract on the blockchain via the Mininet infrastructure.

Blockchain Integration: Ganache is configured to simulate a local Ethereum blockchain. A smart contract deployed on Ganache verifies the ZKP and logs authentication events, including vehicle IDs (anonymized) and timestamps.

To assess the effectiveness of the proposed framework, the following metrics are measured: Performance was measured through authentication latency and throughput. Here, authentication latency was defined as the time to generate, submit, and verify ZKP-OTP proofs. Throughput measures the number of successful authentication events processed per second.

Scalability was measured using vehicle density and infrastructure load. Vehicle density measured the impact of increasing the number of vehicles on authentication latency and throughput. Infrastructure Load measures resource utilization of RSUs and blockchain nodes during peak traffic scenarios. Privacy was assessed through measures of information leakage and replay protection. The information Leakage measure examined data exposed during authentication to ensure no sensitive information (e.g., vehicle identity) is revealed. The replay protection measure provided validation of OTP mechanisms to prevent replay attacks. Energy Efficiency was measured through computational resource consumption during ZKP generation and verification, as well as through the energy usage of blockchain nodes for smart contract execution.

• Baseline Authentication: Vehicles authenticate using traditional PKI-based methods to establish a baseline for comparison.
• ZKP-OTP Authentication: The proposed ZKP-OTP framework is evaluated under identical conditions.
• Scalability Testing: Vehicle density is increased incrementally (e.g., 100, 200, 500 vehicles), and performance metrics are recorded.
• Stress Testing: Simultaneous authentication requests from multiple vehicles are generated to evaluate system robustness under heavy load.

Data Logging: Authentication events, timestamps, and proof verification outcomes are logged to the blockchain. Vehicle-RSU interaction logs are captured using TraCI and Mininet scripts.
Visualization: Performance metrics are visualized using Matplotlib and Pandas. Blockchain logs are analyzed to assess system integrity and event consistency.
Comparative Analysis: Results from the ZKP-OTP framework are compared against baseline methods to highlight improvements in privacy, performance, and scalability.

This experimental setup ensures a comprehensive evaluation of the proposed framework in a controlled yet realistic environment, offering insights into its applicability and robustness in real-world ITS scenarios.