Email: [patents@cumail.in](mailto:patents@cumail.in),

**INVENTOR DETAIL:**

**NAME: Rahul**

**GENDER: Male**

**EMAIL: rahul.es2024@gmail.com**

**MOBILE NO: +91 9814911141**

**DEPARTMENT: Apex Institute of Technology**

**DESIGNATION: Student**



**SCANNED HAND SIGNATURE**

A) Please enlist the **Key concepts and terms/Keywords/Synonyms used in the Invention**?

|  |  |  |
| --- | --- | --- |
| **S. No** | **Keywords for invention** | **Synonyms** |
| 1 | Federated Learning | Collaborative Machine Learning, Distributed ML |
| 2 | Zero-Knowledge Proofs | ZKP, Cryptographic Proofs, Privacy-Preserving Verification |
| 3 | Ephemeral Tokens | Short-lived Tokens, Temporary Cryptographic Tokens |
| 4 | Multi-Modal Sensor Fusion | Sensor Data Integration, Heterogeneous Sensor Processing |
| 5 | Vehicle-to-Infrastructure | V2X Communication, DSRC, C-V2X |
| 6 | Differential Privacy | Privacy-Preserving Data Analysis, Noise Addition |
| 7 | Blockchain Audit Trail | Immutable Ledger, Distributed Audit Log |
| 8 | Trusted Execution Environment | TEE, Hardware Security Module, Secure Enclave |
| 9 | Pseudonym Rotation | Identity Obfuscation, Privacy Rotation |
| 10 | Toll Collection System | Electronic Tolling, Smart Toll, Automated Billing |

**Written Description - Invention Information**

# 1. TITLE OF INVENTION

|  |
| --- |
| Ephemeral Federated Multi-Modal Tolling System |

# 2. BACKGROUND OF THE INVENTION

|  |
| --- |
| Traditional electronic toll collection (ETC) systems face significant privacy and security challenges. Existing systems typically require vehicles to transmit identifiable information, creating privacy risks and potential for tracking. Current tolling solutions lack robust auditability and are vulnerable to manipulation. Prior art in federated learning for IoT applications exists, but no system combines ephemeral tokens, zero-knowledge proofs, multi-modal sensor fusion, and blockchain audit trails specifically for toll collection while maintaining privacy.  The closest prior art includes:   * Traditional ETC systems (e.g., E-ZPass) that require persistent vehicle identification * Basic federated learning implementations in healthcare/telecom, but not adapted for real-time tolling * Blockchain-based audit systems without privacy preservation * Sensor fusion systems without cryptographic privacy guarantees   This invention overcomes these limitations by creating a comprehensive privacy-preserving tolling ecosystem that enables accurate toll collection while protecting user privacy through cryptographic means. |

# 3. BRIEF SUMMARY OF INVENTION

|  |
| --- |
| The Ephemeral Federated Multi-Modal Tolling (EFMM-Toll) system is a novel privacy-preserving electronic toll collection solution that integrates four key technologies: (1) Multi-modal sensor fusion for accurate vehicle detection, (2) Federated learning for collaborative model improvement without data sharing, (3) Zero-knowledge proofs for privacy-preserving payment verification, and (4) Blockchain-based audit trails with TEE attestations. The system uses ephemeral tokens for secure communications and implements differential privacy and pseudonym rotation to protect user identities. Unlike traditional tolling systems, EFMM-Toll enables accurate toll collection while providing cryptographic guarantees of privacy and auditability. |

**4. OBJECTIVE OF THE INVENTION**

|  |
| --- |
| The primary objective is to create a toll collection system that:   * Enables accurate vehicle detection and toll calculation without compromising user privacy * Provides cryptographic proof of payment without revealing financial details * Maintains immutable audit trails for regulatory compliance * Enables collaborative model improvement through federated learning * Prevents long-term tracking of vehicles through ephemeral identities * Ensures system integrity through hardware-based security (TEE) * Scales to handle millions of transactions while maintaining privacy guarantees |

# 5. EXPLAIN PROBLEMS IN PRIOR ART OR EARLIER INVENTION WHICH YOUR PRESENT INVENTION TARGET TO SOLVE POINTWISE.

1. **Privacy Invasion**: Traditional ETC systems require persistent vehicle identification, enabling tracking and profiling of driver behaviour and locations.
2. **Lack of Auditability**: Existing systems lack immutable audit trails, making them vulnerable to manipulation and disputes.
3. **Data Centralization**: Conventional tolling systems collect all data in central repositories, creating single points of failure and privacy risks.
4. **Limited Accuracy**: Single-sensor systems are prone to false positives/negatives, especially in adverse weather conditions.
5. **Scalability Issues**: Centralized ML model training requires massive data transfers and computational resources.
6. **Payment Privacy**: Current systems reveal payment amounts and balances, enabling financial profiling.
7. **Identity Linkability**: Vehicle identities can be linked across multiple toll transactions, compromising privacy.
8. **System Manipulation**: Lack of cryptographic proofs makes systems vulnerable to fraud and manipulation.
9. **Regulatory Compliance**: Existing systems struggle to provide verifiable audit trails for regulatory oversight.
10. **Edge Computing Limitations**: Traditional systems don't leverage edge computing for real-time privacy-preserving processing.

# 6. NOVEL ASPECTS OF THE INVENTION (Point out the new parts used in the invention which make it different from the other existing inventions or prior arts).

|  |
| --- |
| 1. **Integrated Privacy-Preserving Architecture**: Unlike traditional ETC systems that sacrifice privacy for functionality, EFMM-Toll uniquely integrates four technologies (federated learning, zero-knowledge proofs, blockchain audit trails, and multi-modal sensor fusion) into a cohesive privacy-preserving tolling ecosystem, providing mathematical guarantees of privacy while maintaining system accuracy. 2. **Ephemeral Token System**: The invention introduces short-lived cryptographic tokens (maximum 5 minutes) that prevent long-term vehicle tracking, unlike persistent identifiers used in systems like E-ZPass or TollTag, enabling privacy-preserving toll collection without sacrificing transaction security. 3. **Zero-Knowledge Payment Verification**: The system employs zero-knowledge proofs for toll payment verification, allowing proof of payment validity without revealing actual payment amounts or account balances, a novel application of ZKP technology specifically adapted for real-time tolling transactions. 4. **Hardware-Backed Privacy Enforcement**: Integration of Trusted Execution Environments (TEE) for payment verification ensures that even system administrators cannot access sensitive payment data, providing hardware-enforced privacy guarantees not found in software-only tolling systems. 5. **Differential Privacy in Tolling**: Application of differential privacy (ε=1.0, δ=1e-5) to location data and sensor readings in toll collection systems, enabling collaborative model improvement while providing formal privacy guarantees against re-identification attacks. 6. **Automated Pseudonym Rotation**: Vehicles automatically rotate their cryptographic pseudonyms every hour, preventing correlation of toll transactions across time periods, unlike static vehicle identifiers in existing tolling infrastructure. 7. **Real-Time Federated Learning for Toll Accuracy**: The system continuously improves vehicle detection accuracy through federated learning without sharing raw sensor data, enabling collaborative model training across distributed RSUs while maintaining data locality and privacy. 8. **Blockchain Audit Trails with TEE Attestation**: Combining blockchain technology with hardware-based attestations for audit records, providing immutable, hardware-verified audit trails that cannot be manipulated even by privileged system operators. 9. **Multi-Modal Sensor Fusion with Privacy Preservation**: Advanced ML-based sensor fusion combining camera, LiDAR, and radar data with built-in differential privacy mechanisms, enabling robust vehicle detection in adverse conditions while protecting sensor data privacy. 10. **V2X Communication with Cryptographic Privacy**: Secure vehicle-to-infrastructure communication protocols that maintain privacy through ephemeral keys and zero-knowledge proofs, unlike existing V2X systems that often transmit identifiable vehicle information. 11. **Distributed Trust Model**: The four-component architecture (RSU Edge, Vehicle OBU, Federated Aggregator, Distributed Ledger) creates a decentralized trust model where no single component can compromise system privacy or integrity. 12. **Mathematical Privacy Guarantees**: The system provides formal cryptographic proofs of privacy preservation, enabling toll collection with quantifiable privacy assurances (ε-differential privacy bounds) rather than relying on policy-based privacy protection. |

**7. DETAILED DESCRIPTION OF THE INVENTION** - ***Be sure to use as much space as needed, and be as detailed as you can in this section, as anything that is not covered here will not be protected under the patent we may obtain.***

***\*\*\*Note: please explain your invention step wise in sequential order and how it works and duly explain all the parts of the device in sequential order with its functionality****.*

*In case of software embedded with device; - explain step wise how the software works with the device and its functionality, with flow chart and diagram. \*\*\**

|  |
| --- |
| The EFMM-Toll system consists of four interconnected services deployed across roadside infrastructure and vehicles:  **System Architecture:**  **RSU Edge Module (Roadside Unit):**   * **Sensor Adapters**: Interface with cameras, LiDAR, radar sensors * **Fusion Engine**: Combines multi-modal sensor data using ML for vehicle detection * **Token Orchestrator**: Generates ephemeral tokens for secure vehicle interaction * **Payment Verifier**: Validates ZKP payment proofs using TEE * **FL Client**: Participates in federated learning rounds * **Audit Buffer**: Local audit record storage before blockchain submission   **Vehicle OBU App (On-Board Unit):**   * **V2X Client**: Handles vehicle-to-infrastructure communication * **Token Holder**: Manages ephemeral tokens received from RSUs * **Wallet**: Generates ZKP payment proofs without revealing balance * **Privacy Manager**: Implements pseudonym rotation and location anonymization * **FL Client**: Contributes to federated model improvement   **Federated Aggregator Service:**   * **Aggregation Server**: Coordinates FL rounds across RSUs and vehicles * **Model Repository**: Versioned storage of ML models * **Privacy Engine**: Applies differential privacy to model updates * **Participant Registry**: Manages RSU and vehicle registrations   **Distributed Audit Ledger:**   * **Ledger Node**: Implements blockchain consensus * **Attestation Manager**: Handles TEE-based attestations * **Consensus Engine**: Ensures distributed agreement * **Audit Verifier**: Provides query interface for audit records   **Operational Flow:**   1. Vehicle approaches toll zone 2. RSU sensors detect vehicle using multi-modal fusion 3. RSU generates ephemeral token with toll challenge 4. Vehicle receives token via V2X communication 5. Vehicle generates ZKP payment proof 6. RSU verifies proof in TEE environment 7. Transaction recorded in blockchain audit trail 8. Federated learning improves detection models collaboratively   **Privacy Mechanisms:**   * **Ephemeral Tokens**: Short-lived cryptographic tokens (5 minutes default) * **Zero-Knowledge Proofs**: Prove payment validity without revealing amounts * **Differential Privacy**: Adds noise to location and sensor data (ε=1.0, δ=1e-5) * **Pseudonym Rotation**: Changes vehicle identifiers every hour * **TEE Integration**: Hardware-based secure execution for critical operations   **Technical Implementation:**   * **Programming Language**: Python 3.11+ with AsyncIO * **ML Frameworks**: PyTorch, TensorFlow for model training/inference * **Cryptography**: Custom ZKP implementation, AES-256 encryption * **Communication**: V2X (DSRC/C-V2X), HTTP/REST, WebSocket, gRPC * **Deployment**: Docker containers with Kubernetes orchestration * **Database**: SQLite for local buffers, distributed databases for shared state. |

**8. DRAWINGS OR SUPPORT MATERIAL**

|  |
| --- |
| **Figure 1: System Architecture Overview**  **Figure 2: Privacy Protection Layers**  **Figure 3: Toll Collection Sequence** |

# 9. SUMMARY OF THE FIGURES / DIAGRAMS / DRAWINGS with the explanation of all parts in the drawing and how it works.

**Figure 1: System Architecture Overview**  
This diagram shows the four main components of the EFMM-Toll system:

* **RSU Edge Module**: Deployed at toll collection points, handles sensor fusion, token generation, and payment verification
* **Vehicle OBU App**: Installed in vehicles, manages V2X communication, payment proofs, and privacy protection
* **Federated Aggregator Service**: Cloud-based service coordinating federated learning across distributed nodes
* **Distributed Audit Ledger**: Blockchain network providing immutable audit trails  
  The arrows indicate communication protocols (V2X, HTTP/REST, WebSocket, gRPC) used between components.

**Figure 2: Privacy Protection Layers**  
Illustrates the hierarchical trust model:

* **Hardware Root of Trust**: TEE/TPM provides hardware-based security foundation
* **Cryptographic Identity**: PKI certificates establish entity identities
* **Zero-Trust Communications**: Mutual TLS ensures secure inter-component communication
* **Decentralized Verification**: Multi-party consensus prevents single points of failure
* **Cryptographic Proofs**: ZKP and digital signatures provide privacy-preserving verification

**Figure 3: Toll Collection Sequence**  
Shows the end-to-end toll collection process:

1. **Vehicle Approach**: Vehicle enters sensor detection range
2. **Detection**: Multi-modal sensors (camera, LiDAR, radar) capture vehicle data
3. **Sensor Fusion**: ML algorithms combine sensor inputs for accurate detection
4. **Classification**: ML model identifies vehicle type and characteristics
5. **Token Exchange**: RSU generates ephemeral cryptographic token
6. **Ephemeral Token**: Short-lived token prevents long-term tracking
7. **Cryptographic Challenge**: Token contains toll amount and proof requirements
8. **ZK Proof**: Vehicle generates zero-knowledge payment proof
9. **TEE Verify**: RSU validates proof in trusted execution environment
10. **Blockchain**: Transaction recorded in immutable audit ledger

**10. ABSTRACT (150 words)**

The Ephemeral Federated Multi-Modal Tolling (EFMM-Toll) system revolutionizes electronic toll collection by integrating privacy-preserving technologies with advanced sensor fusion and distributed computing. The invention combines four novel components: (1) RSU Edge Module with multi-modal sensor fusion for accurate vehicle detection, (2) Vehicle OBU App with zero-knowledge proof payment verification, (3) Federated Aggregator Service for collaborative model improvement, and (4) Distributed Audit Ledger with TEE attestations. Key innovations include ephemeral tokens preventing long-term tracking, differential privacy protecting location data, pseudonym rotation for identity protection, and blockchain-based audit trails ensuring regulatory compliance. The system enables toll collection with cryptographic privacy guarantees, federated learning for continuous accuracy improvement, and hardware-based security through trusted execution environments. Unlike traditional ETC systems, EFMM-Toll provides mathematical proof of privacy preservation while maintaining transaction accuracy and auditability, addressing critical privacy concerns in intelligent transportation systems.

**11. BRIEF DETAIL OF PARTS OF THE DEVICE, APPARATUS, PRODUCT IN BULLET POINTS – In case the invention is related to product, device and apparatus**.

\*\*\*Note: Explain the Parts of the Device\*\*\*

**RSU Edge Module Components:**

* **Sensor Adapters**: Hardware interfaces for camera (OpenCV), LiDAR (PCL), radar sensors with real-time data normalization
* **Fusion Engine**: PyTorch/TensorFlow-based ML processor combining heterogeneous sensor inputs with confidence scoring
* **Token Orchestrator**: Cryptographic token generator using JWT with ephemeral key pairs and configurable lifetimes
* **Payment Verifier**: TEE-integrated ZKP verification engine with hardware attestation capabilities
* **FL Client**: Federated learning participant with secure model update encryption and differential privacy
* **Audit Buffer**: Local SQLite database with cryptographic hashing for tamper-evident record storage.

**Vehicle OBU App Components:**

* **V2X Client**: DSRC/C-V2X protocol stack with secure key exchange and message authentication
* **Token Holder**: Ephemeral token storage with automatic expiration and secure deletion
* **Wallet**: ZKP payment proof generator using Bulletproofs protocol with balance hiding
* **Privacy Manager**: Location anonymization engine with configurable privacy budgets (ε=1.0, δ=1e-5)
* **FL Client**: Collaborative ML participant with model weight encryption and secure aggregation

**Federated Aggregator Service Components:**

* **Aggregation Server**: FastAPI-based coordination service with round-based FL orchestration
* **Model Repository**: MLflow-integrated versioned storage with model validation and rollback
* **Privacy Engine**: PyDP-based differential privacy application with configurable noise parameters
* **Participant Registry**: PostgreSQL database with entity authentication and reputation tracking

**Distributed Audit Ledger Components:**

* **Ledger Node**: Custom blockchain implementation with PBFT consensus and block validation
* **Attestation Manager**: TPM/TEE integration for hardware-based attestation generation
* **Consensus Engine**: Multi-signature validation with configurable quorum requirements
* **Audit Verifier**: REST API interface for cryptographic proof verification and record retrieval

12. **BRIEFLY EXPLAIN THE STEPS, FLOW CHART, FUNCTIONALITY OF INVENTION RELATED TO SOFTWARE, EMBEDDING WITH MACHINE, DEVICE, APPRATUS.**

\*\*\*Note: Explain the functionality of software embedded with the device\*\*\*

**Software Flow Chart:**

**1. System Initialization**

**↓**

**2. Component Registration (RSU ↔ Aggregator ↔ Ledger)**

**↓**

**3. Federated Learning Round Start**

**↓**

**4. Local Model Training (RSU/OBU)**

**↓**

**5. Privacy-Preserving Update Encryption**

**↓**

**6. Secure Model Aggregation (Differential Privacy)**

**↓**

**7. Global Model Distribution**

**↓**

**8. Vehicle Detection Event**

**↓**

**9. Multi-Modal Sensor Fusion**

**↓**

**10. Ephemeral Token Generation**

**↓**

**11. V2X Token Transmission**

**↓**

**12. Zero-Knowledge Proof Generation**

**↓**

**13. TEE-Based Proof Verification**

**↓**

**14. Blockchain Transaction Recording**

**↓**

**15. Audit Trail Verification**

**↓**

**16. Privacy Budget Update**

**↓**

**17. Pseudonym Rotation (if needed)**

**↓**

**Back to Step 3 (Continuous Learning Loop)**

**Key Software Functionalities:**

1. **AsyncIO Event Loop**: All components use Python AsyncIO for concurrent processing of sensor data, network communications, and ML inference
2. **Federated Learning Coordination**: Flower framework manages distributed model training with secure aggregation
3. **Cryptographic Operations**: Custom ZKP library implements Bulletproofs for payment verification without balance disclosure
4. **TEE Integration**: Intel SGX/AMD SEV SDK provides hardware-isolated execution for sensitive operations
5. **Multi-Modal Fusion**: PyTorch-based neural networks combine camera, LiDAR, and radar data for robust detection
6. **Blockchain Consensus**: Custom PBFT implementation ensures distributed agreement on audit records
7. **Differential Privacy**: PyDP library adds calibrated noise to model updates and location data
8. **V2X Protocol Stack**: Custom DSRC/C-V2X implementation with security extensions for tolling

**13. BRIEFLY EXPLAIN THE STEPS OF PROCESS, COMPOSITION IN BULLET POINTS – In case the invention is related to process, composition.**

**\*\*\*Note: Ignore it if the invention is not related to process, composition\*\*\***

**Toll Collection Process:**

* Vehicle enters sensor detection zone (100-500m range)
* Multi-modal sensors capture vehicle data simultaneously (camera frames, LiDAR point clouds, radar reflections)
* Sensor fusion engine combines inputs using ML model for vehicle classification and confidence scoring
* RSU generates ephemeral token with toll amount and cryptographic challenge
* Token transmitted via V2X secure channel to vehicle OBU
* Vehicle wallet generates zero-knowledge proof of sufficient balance
* Payment proof sent back to RSU via V2X
* RSU verifies proof in TEE without learning payment details
* Successful verification triggers toll gate opening
* Transaction recorded in local audit buffer
* Audit records batched and submitted to blockchain network
* Consensus achieved across distributed ledger nodes
* Immutable audit trail established for regulatory compliance

**Federated Learning Process:**

* Aggregator initiates new training round with global model parameters
* RSUs and OBUs receive model update notifications
* Local training performed on private sensor/payment data
* Model weight updates encrypted with differential privacy noise
* Updates securely transmitted to aggregator via TLS
* Aggregator collects updates from minimum participant threshold
* Secure aggregation performed using privacy-preserving techniques
* Global model updated and validated
* New model distributed to all participants
* Local models updated with global weights
* Process repeats continuously for model improvement

**Privacy Protection Process:**

* Vehicle location data processed through differential privacy filter (ε=1.0, δ=1e-5)
* Pseudonyms rotated every 3600 seconds to prevent long-term tracking
* Ephemeral tokens expire after 300 seconds maximum
* All communications use mutual TLS with certificate pinning
* Sensitive data encrypted with AES-256 before storage/transmission
* TEE provides hardware-based execution guarantees for verification
* Zero-knowledge proofs ensure payment validity without balance disclosure

**14. RELATED PUBLICATION (If Any)**

None - This is a novel invention combining previously separate technologies in a unique way for toll collection applications.