AUTONOMOUS TRAFFIC POLICE MANAGEMENT SYSTEM

25-26J-300

Project Proposal Report

Y.G.Y Induwara

B.Sc. (Hons) Information Technology

Faculty of Computing

Sri Lanka Institute of Information Technology
Sri Lanka

August 2025

DECLARATION

I declare that this proposal is my own work and does not incorporate, without acknowledgement, any material previously submitted for a degree or diploma in any other University or Institute of higher learning; to the best of my knowledge it does not contain any material previously published or written by another person except where due acknowledgement is made in the text.

Name	Student ID	Signature	Date
Y.G.Y. Induwara	IT22601056		30/08/2025

The above candidate is carrying out research for the undergraduate Dissertation under my supervision.

Name	Role	Signature	Date
Mr. Ravi Supunya	Supervisor		
Ms.Dulani Jayasinghe	Co - Supervisor		

ABSTRACT

Traffic offences have become an increasingly significant problem in cities, contributing to road congestion, causing accidents, and making roads less safe. The conventional method of enforcement is usually ineffective, haphazard, and has no predictive qualities. The proposed platform integrates blockchain technology for immutable record-keeping and IPFS-based decentralized storage to ensure evidence integrity. AI driven tools provide verification of uploaded media if the media was AI generated or not, and ZKPs cryptographic technique-based system to witness protection in the legal process to increase the efficiency and security of the case related data and legal cases. The methodology assumes data collection using traffic cameras, LPR systems, and violation records, as well as the AI-based models of decision-making when assigning tasks and predictive analysis. The accuracy, efficiency, and effectiveness of using the system to deal with violations will be validated by simulation testing. The anticipated results are enhanced enforcement speed, decreased officer workload, and enhanced the security of evidence management system in Bar related cases. In this research project, I expect to use Python, React, Zero Knowledge Proofs (ZKPs), Ethereum, MSSQL, and Interplanetary File System (IPFS) as the main key technologies. The originality of the current study is the unparalleled integration of historical investigation, real-time investigation, and predictive policing, which allowed the introduction of law enforcement authorities to transition to the so-called proactive prevention as opposed to the reactive one. The system also offers a contemporary solution to road safety and improves empowers traffic laws by combining AI-driven technologies and automated enforcement.

Contents

DECLARATION 2
ABSTRACT 3
1. Introduction 5
1.1 Background & Literature Survey 5
1.2 Research Gap 6
1.3 Research Problem 7
2. Objectives 8
2.1 Main Objectives 8
2.2 Specific Objectives 8
3. Methodology 10
3.1 Research Design 10
3.2 Overall Component Description 10
3.3 Overall System Architecture 11
3.4 Component Specific System Architecture Diagram 12
3.4 Workflow & Data Flow 12
4. Project requirements 13
4.1 Functional requirements 13
4.2 Non-Functional Requirements 13
4.3 User & System Requirements 13
Budget and Budget Justification 13
Project Gantt Chart 14
References 15
Appendices 15

1. Introduction

1.1 Background & Literature Survey

Sri Lanka's law enforcement and traffic management systems face significant and persistent challenges those days because of the inefficient processes, outdated manual operations, and a general lack of transparency. Current procedures depend heavily on human based manual activities. Evidence collection, fine issuance, and traffic violation management, which not only slows down legal proceedings but also increases human errors and other unexpected errors. Because of these inefficiencies lead to delays in legal judgments, difficulties in handling digital and physical evidence. And also provide opportunities for corruption and unauthorized manipulation of case related data in some cases. Moreover, the absence of a centralized, secure, and automated platform for traffic offense management makes several barriers for both law enforcement of authorities and citizens. Without such a system, storing the data and accessing legal evidence such as video footage, witness testimonies, and traffic reports remains prone to tampering, ability to lose, and unauthorized access, resulting in reduced public trust in the system.

Researchers worldwide have researched cutting edge technologies like blockchain, artificial intelligence, and decentralized storage methods to solve these obstacles. Zhao and Tan [1] who were the researchers researched and implemented a Blockchain based Digital Chain of Custody system for multimedia evidence management. Their suggested approach uses for cryptographic hashing in conjunction with blockchain's immutable ledger capabilities to guarantee data authenticity and integrity. Their work addresses the requirement for a tamperproof audit trail, which is essential in legal context, by keeping a verifiable record of all actions taken on multimedia files.

Similarly, to securely and effectively handle massive amounts of evidence, Li and Kim [2] suggested an advanced court evidence preservation scheme that combines blockchain technology with the Inter Planetary File System (IPFS). According to their idea, blockchain stores immutable content hashes to ensure authenticity and traceability, while IPFS is utilized for decentralized off-chain storage. This combination makes it appropriate for court authorities managing big databases of digital evidence since it guarantees scalable storage, effective retrieval, and integrity verification.

These studies are mostly focused on judicial settings and are not made to help real-time law enforcement operations, even though they show notable advancements in secure evidence retention. Critical features like automated traffic violation detection, immediate fine administration, and AI-powered legal aid for both civilians and law enforcement are usually not covered by current systems. Additionally, none of the strategies examined incorporate real-time dashboards or predictive analytics to enhance resource allocation and traffic management effectiveness.

This research builds on the developments made by Li and Kim [2] and Zhao and Tan [1] by proposing a Blockchain-Based Secure Evidence & Legal Dossier System that is coupled with real-time traffic enforcement mechanisms and AI-driven decision-support tools. In contrast to current solutions, the suggested solution offers a full platform for Sri Lanka's traffic law enforcement by fusing the immutability of blockchain technology with the decentralized storage of IPFS and automation driven by artificial intelligence. Predictive dashboards to help officers optimize traffic flow and patrol duty distribution, WhatsApp and SMS connection for fast fine notifications, and license plate recognition (LPR) for automatic violation identification are all features of the system.

The proposed framework seeks to improve the overall experience of citizens interacting with traffic authorities by reducing corruption, increasing operational efficiency, and promoting transparency. This research aims to provide a contemporary, citizen-centric paradigm for traffic management and legal evidence processing in Sri Lanka by developing a safe, scalable, and intelligent platform. This will help to create a more transparent legal environment and reliable digital government.

1.2 Research Gap

At the current situation globally adoption of blockchain and AI in legal evidence management and smart policing but in Sri Lanka lacks a centralized, secure, and transparent platform for traffic enforcement. Referred literature shows that below things in different countries used in the world.

- Blockchain to secure court records system using in Estonia
- LPR-based AI systems for real-time violation detection integrates by Singapore Police
- India’s Delhi Police employs AI dashboards for predictive traffic analytics.

But in Sri Lanka, there are no integrated solution combining blockchain, AI powered legal intelligence, and decentralized evidence storage tailored to Sri Lanka’s environment. Also, there is lot of research related to Blockchain development and AI Integration research in different research in the world. In that research, I could have to find Li and Kim [2] and Zhao and Tan [1] by proposing a Blockchain-Based Secure Evidence & Legal Dossier System that is coupled with real-time traffic enforcement mechanisms and AI-driven decision-support tools. These tools called singularity of the issues in police officers faced but there is no system to Evidence management with block chain, AI verification and ZKPs powered witness protection feature included system in all over the world. So that I could have to identify this as a research gap of my research.

1.3 Research Problem

Most of judicial cases in Sri Lanka disqualified because of the not enough evidence to prove against the defendant. Sometimes the evidence intentionally dismissed by police officers because of the effect from higher officers and political interaction sometimes evidence is destroyed due to officers' mistakes.

Because of those reasons, I tried address the core question using this research project is "How can emerging technologies (blockchain, AI, and automation) optimize transparency, reduce corruption, and enhance operational efficiency in Sri Lanka's traffic police department and traffic police law enforcement?"

2. Objectives

2.1 Main Objectives

Main purpose is to develop a secure and decentralized platform integrated with block chain for improve the security and AI verification media to avoid upload deepfake media as a evidence and finally automate and enhance Sri Lanka traffic police related law enforcement is the main objective in this project.

2.2 Specific Objectives

Prior work shows that blockchain can strengthen evidentiary integrity by recording an immutable chain of custody and anchoring content hashes for later verification (e.g., multimedia custody frameworks and blockchain–IPFS preservation schemes in [1], [2]). However, three critical gaps remain for a solution that must operate as a practical, end-to-end *secure evidence vault* for Sri Lanka's context:

(1) Evidence Vault beyond "hash on chain":

Existing studies typically secure *proof* of evidence (hashes, timestamps, transfer logs) while storing the bulk content off-chain. They do not fully specify a production-grade vault with fine-grained, revocable access control; multi-party custody workflows (capture → seal → review → disclose); key-management/rotation for long-lived legal retention; lawful unsealing and redaction processes; and provenance standards (e.g., side-channel metadata integrity, device attestation). There is limited guidance on mobile/field ingestion under intermittent connectivity, chain re-org risk, and cost/latency trade-offs for high-volume media typical of policing. Thus, a gap exists in designing a *complete lifecycle* vault that integrates blockchain immutability with operational controls, human factors, and admissibility requirements not merely hash anchoring [1], [2].

(2) Anonymous Witness Protection using Zero Knowledge Proofs (ZKPs)

While anonymity and whistle blower protections are well discussed conceptually, prior blockchain evidence systems rarely apply *practical ZKPs* to allow witnesses to prove eligibility, presence, or relationship to an event without disclosing identity. Open questions include issuer agnostic credentialing (e.g., selective disclosure from verifiable credentials), Sybil resistance without deanonymizing users, revocation that preserves anonymity, link ability limits across submissions, and court-compatible audit trails that remain privacy-preserving. There is a clear gap in protocols and data models that combine with anonymous

submission, verifiable, non-repudiable attestations; and controlled de anonymization under judicial order within a single evidence workflow.

(3) AI Authenticity/Deepfake Verification that is legally interpretable and robust

Media forensics has progressed rapidly, but most detectors are brittle to compression, re-encoding, post processing, domain shift, and adversarial attacks; many are trained on English/Chinese datasets and do not generalize to Sinhala/Tamil speech or regional visual contexts. Few systems tie detector outputs to provenance claims (e.g., capture-device attestations, C2PA-style manifests) and anchor those claims in a tamper-evident ledger for courtroom scrutiny. Critically, current work seldom provides legally interpretable reports calibrated confidence, error bounds, methodology transparency, and reproducible pipelines linked to chain-of-custody entries. The gap is a forensically rigorous, multilingual, and auditable AI verification layer that couple's detection with provenance and on-chain accountability.
Integration gap across the three pillars:
No prior system unifies (a) a *lifecycle-complete* blockchain evidence vault, (b) *ZKP-based* anonymous-yet-verifiable witness workflows, and (c) *court-ready* AI authenticity assessments under one coherent architecture aligned to local operational constraints, privacy laws, and evidentiary standards. This absence of an integrated, privacy-preserving, and explainable framework constitutes the core research gap that your project addresses, extending beyond the scope of existing blockchain custody and preservation approaches [1], [2].

3. Methodology

3.1 Research Design

This project follows Design Science Research Methodology (DSRM). This methodology is more appropriate to develop and evaluate innovative technological frameworks. In my research solution is expected to be conveyed into the following phases.

1. Identify the Problem
    - Conducted a detailed study of Sri Lanka's current traffic law enforcement and evidence management workflows.
    - Identified inefficiencies, lack of transparency, and absence of secure storage mechanisms.
2. Requirement Gathering phase
    - Consulted traffic police officers, legal experts, and technical stakeholders in Sri Lanka
    - Analyzed existing frameworks and evidence and related laws.
3. Expected System Design & Architecture
    - Designed a practical architecture integrating blockchain, IPFS, ZKPs, and AI-based media verification.
4. Create a prototype
    - Implement a secure blockchain evidence vault.
    - Integrate AI deepfake detection and ZKP-based witness protection modules for the system
    - Connect the platform with other components.
5. QA phase
    - Test the system with the use of synthetic datasets and real world traffic videos.
    - Conduct performance, scalability, usability and vulnerability assessments and get the actions if needed.

3.2 Overall Component Description

The proposed system consists of four tightly integrated layers:

1. Blockchain-Based Evidence Vault

- Stores cryptographic hashes and metadata of evidence on-chain.
- Uses IPFS to handle large files like videos and images efficiently.
- Ensures immutability, traceability, and multi-party access control.

2. Zero-Knowledge Proof (ZKP) Witness Protection
    - Enables anonymous witness submissions while maintaining verifiability.
    - Allow selective disclosure under judicial orders without revealing identities unnecessarily.
    - Uses non-interactive ZKP protocols for efficiency and scalability.
3. AI Authenticity Verification Module
    - Uses deep learning-based forensic analysis to detect deepfakes or manipulated content.
    - Incorporates explainable AI (XAI) methods to provide legally admissible reports.
    - Anchors verification results on the blockchain for tamper-proof auditability.

3.3 Overall System Architecture

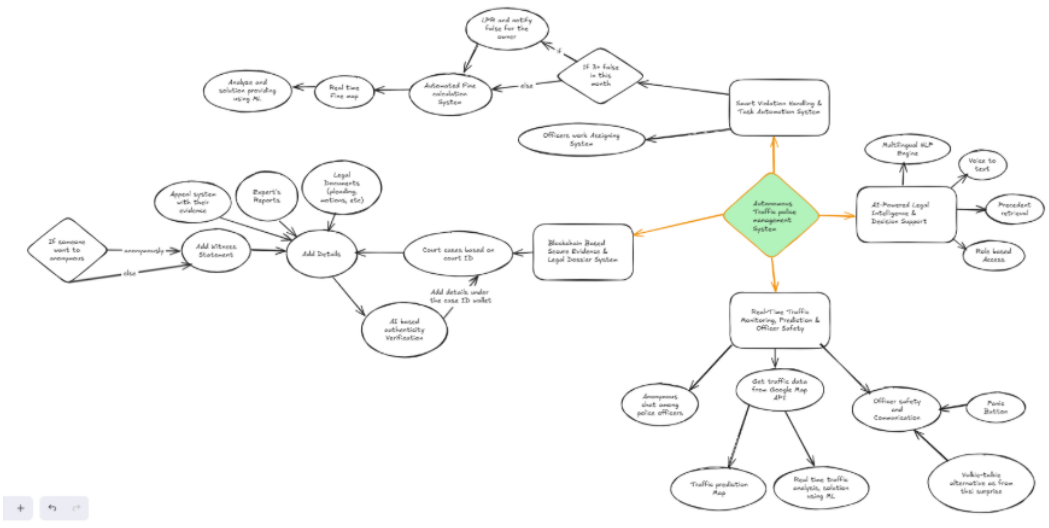

Figure 1 :Overall System Architecture

3.4 Component Specific System Architecture Diagram

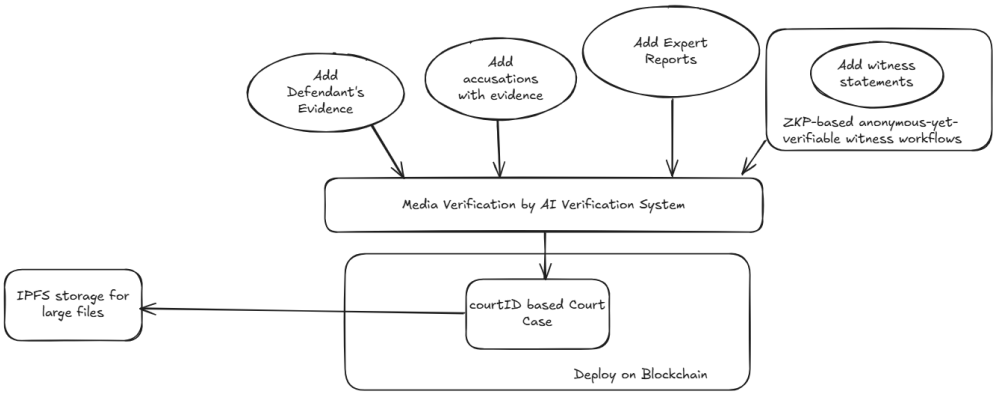

Figure 2: Component Specific System Architecture

3.4 Workflow & Data Flow

Below is how the process works end to end happens.

1. Collection → Evidence is uploaded via police, cameras, or citizen witnesses.
2. Anonymous Submissions → Witnesses can submit without revealing identity using ZKPs.
3. Verification → AI module checks authenticity (real vs. deepfake).
4. Anchoring → Metadata and hashes are stored immutably on blockchain; full files go to IPFS.
5. Legal Proceedings → Courts access tamper-proof records with chain-of-custody evidence.

4. Project requirements

4.1 Functional requirements

- Evidence uploads, encryption, and IPFS storage works properly.
- Violation detection and automated fine issuance.
- Integration with WhatsApp API for notifications.
- Role-based dashboards for police, legal officers, and citizens.

4.2 Non-Functional Requirements

- Security (High security requirement for the data)
- Scalability
- Availability (99% uptime)
- Interoperability
- Fast access to the system

4.3 User & System Requirements

- Web Access for officers and citizens.
- Provide enhanced security for the legal cases data
- Protect witness from ZKPs Technology.
- APIs for integration with other ATPMS components.

Budget and Budget Justification

Component	**Cost (LKR)**	**Justification**
Blockchain Nodes	250,000	Decentralized ledger
AI Training Models	180,000	Multilingual assistant
LPR Hardware	400,000	High-accuracy detection
Cloud Infrastructure	120,000	Hosting & API gateway

Figure 3: The budget allocation table

Project Gantt Chart

Task / Phase	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep
1. Project Planning & Requirement Analysis												
2. Data Gathering												
3. Blockchain Development												
4. Case Retrieval Module												
5. AI verification Development												
6. Integration with ATPMS												
7. User Interface Development												
8. Testing & Evaluation												
9. Feedback & Iterative Improvement												
10. Documentation & Final Evaluation												
11. Final Report Submission												

References

[1] Y. Zhao and K. Tan, "Blockchain-Based Digital Chain of Custody for Multimedia Evidence," *IEEE Trans. Inf. Forensics Security*, vol. 18, no. 2, pp. 845–856, Feb. 2023.

[2] J. Li and S. Kim, "A Study of a Blockchain-Based Judicial Evidence Preservation Scheme," *IEEE Access*, vol. 12, pp. 30214–30225, Mar. 2024.

Appendices