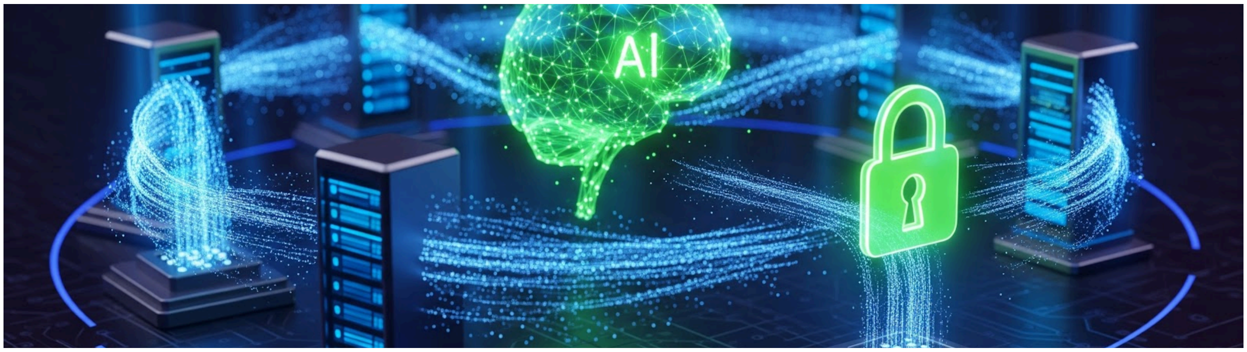


Mine-Safe India: AI-Orchestrated Secure Data Deletion, Migration & Forensic Certification Platform

I. Project Information

Title	Mine-Safe India: AI-Driven No-Wipe Secure Data Migration & Forensic Verification Platform

II. Proposal Details

Problem Statement

The Indian e-waste sector operates on a flawed “Custody-First, Wipe-Later” model. Consumers hand over functional devices containing live Personally Identifiable Information (PII) such as banking tokens and identity data to collection agents, but data destruction occurs only 7–10 days later at centralized warehouses. This creates a critical “Logistics-Gap Vulnerability”—a 168+ hour exposure window during which data is vulnerable to theft, cloning, or misuse during transit. This gap results in high consumer data anxiety and creates significant legal and compliance liability for recyclers, as no verifiable proof of deletion or secure handling exists at the point of handover.

Objective

To design and deploy an AI-driven secure data handling platform that allows users, at the point of device handover, to choose between **verifiable data deletion** or **secure encrypted data migration**, while ensuring forensic verification and regulatory compliance.

- **Delete:** Immediate, cryptographically verifiable data destruction (wipe-first path)
- **Migrate:** Securely transfer device data to a company-controlled server using encryption
- **Verify:** Perform read-only forensic analysis on the original device
- **Certify:** Generate a QR-based, publicly verifiable certificate

Proposed Solution

Mine-Safe India is a **dual-path AI-driven platform** that dynamically executes either a **secure data deletion workflow** or a **secure data migration workflow**, based on **explicit user consent at the point of device collection**.

- **Secure Migration Engine:** Encrypts and transfers device data to a controlled server environment prior to any further analysis, ensuring zero data loss and secure custody.
- **Secure Deletion Engine:** Performs immediate, verifiable data destruction at the collection point, eliminating the logistics-gap vulnerability.
- **Forensic Verification Module:** Conducts **read-only, non-destructive scans** to detect recoverable data, metadata remnants, and storage anomalies, validating the effectiveness of deletion or migration.
- **AI Reasoning Layer (Agentic RAG):** An autonomous AI agent orchestrates multi-step workflows, retrieves contextual evidence from a vector database, and uses Large Language Models (LLMs) to generate **explainable, compliance-aware assessments**.
- **Trust & Certification Layer:** Issues digitally signed certificates with **QR-based public verification**, closing the audit, trust, and liability gap.

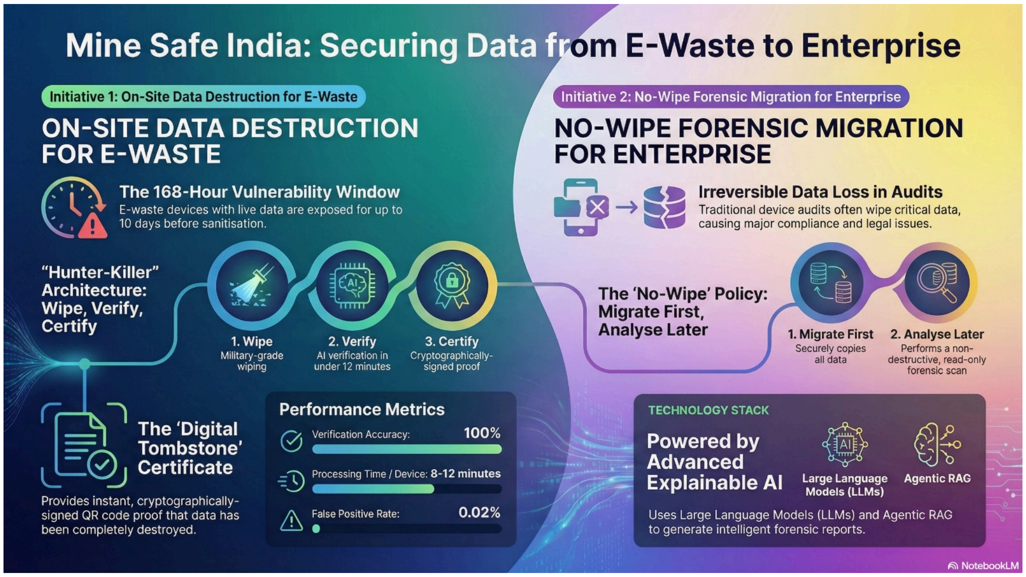
Approach and Methodology

The platform's development is grounded in **secure system design** and **AI governance principles**, strictly adhering to **forensic best practices** and relevant regulatory standards. The implementation is structured into five distinct phases:

Phase	Core Functionality

Phase 1	**Secure Data Handling:** Executes a user-driven choice: either **secure data migration** (using AES-256 encryption with integrity hashing) or **immediate, verifiable data deletion** at the point of collection.
Phase 2	**Forensic Verification:** Implements a read-only forensic scan pipeline to **verify data recoverability** and assess the integrity of the storage medium.
Phase 3	**Content Traceability:** Generates data **embeddings** and integrates them into a **vector database** for fine-grained, content-level data verification and detailed audit logging.
Phase 4	**Intelligent Workflow:** Deploys an **Agentic RAG (Retrieval-Augmented Generation) system**, utilizing structured, MCP-aligned prompts for intelligent workflow orchestration and robust compliance reasoning.
Phase 5	**Audit & Trust Closure:** Generates **official certificates** and enables **QR-based verification and audit validation** to definitively address the trust and liability gap.

Architecture


Mine Safe India: Securing Data from E-Waste to Enterprise
Initiative 1: On-Site Data Destruction for E-Waste
ON-SITE DATA DESTRUCTION FOR E-WASTE
The 168-Hour Vulnerability Window
E-waste devices with live data are exposed for up to 10 days before sanitisation.
"Hunter-Killer" Architecture: Wipe, Verify, Certify
1. Wipe
Military-grade wiping
2. Verify
AI verification in under 12 minutes
3. Certify
Cryptographically-signed proof
The 'Digital Tombstone' Certificate
Provides instant, cryptographically-signed QR code proof that data has been completely destroyed.
Performance Metrics
Verification Accuracy: 100%
Processing Time / Device: 8-12 minutes
False Positive Rate: 0.02%
Initiative 2: No-Wipe Forensic Migration for Enterprise
NO-WIPE FORENSIC MIGRATION FOR ENTERPRISE
Irreversible Data Loss in Audits
Traditional device audits often wipe critical data, causing major compliance and legal issues.
The 'No-Wipe' Policy: Migrate First, Analyse Later
1. Migrate First
Securely copies all data
2. Analyse Later
Performs a non-destructive, read-only forensic scan
TECHNOLOGY STACK
Powered by Advanced Explainable AI
AI
Large Language Models (LLMs)
Agentic RAG
Uses Large Language Models (LLMs) and Agentic RAG to generate intelligent forensic reports.
NotebookLM

The system adopts a Web-Based Agentic Architecture. The frontend provides a live terminal-style interface for operators, while the backend manages secure storage, forensic workflows, and AI reasoning. The AI Agent coordinates tools for migration, scanning, retrieval, and analysis using Model Context Protocol (MCP) to ensure controlled and explainable decision-making. A vector database stores historical forensic embeddings to support Retrieval-Augmented Generation.

Tech Stack

Programming Language: Python 3.10+
LLM Orchestration: Large Language Models (abstracted) used for multi-step reasoning and agent coordination
Embeddings: Sentence Transformers
Vector Database: ChromaDB / FAISS (for embedding indexing and similarity checks)
Backend Framework: FastAPI (API abstraction for migration, vault, and verification services)
Frontend: Streamlit (web-based control and monitoring UI)
Security & Cryptography: AES-256-GCM encryption, cryptographic hashing (SHA-256), QR-based certificate generation
Forensics & Verification: Entropy analysis, signature detection aligned with NIST 800-88 concepts
Platform & Execution Environment: Replit (cloud-based development and execution environment used to simulate and validate the end-to-end AI-orchestrated data lifecycle)
Cloud / Storage Integration: API-abstracted secure vault layer (compatible with AWS S3, private cloud storage, or enterprise servers)
Standards Referenced: NIST 800-88, ISO 27001, DPDP Act 2023**Mine-Safe India:**
AI-Driven No-Wipe Secure Data Migration & Forensic Verification Platform

Core Technology Stack:

- **Programming Language:** Python 3.10+
- **LLM & AI Orchestration:** Utilizes Large Language Models for complex multi-step reasoning and coordinating agent activities.
- **Embeddings & Indexing:** Sentence Transformers for generating embeddings, with ChromaDB / FAISS serving as the Vector Database for efficient indexing and similarity checks.

Platform Architecture & Frameworks:

- **Backend:** FastAPI provides the API abstraction layer for critical services, including data migration, secure vault operations, and forensic verification.
- **Frontend/UI:** Streamlit offers a web-based interface for platform control and real-time monitoring.
- **Execution Environment:** Replit is used as the cloud-based platform to simulate and validate the complete AI-orchestrated data lifecycle.

Security, Forensics, and Compliance:

- **Security & Cryptography:** Implements robust security measures including AES-256-GCM encryption, SHA-256 cryptographic hashing, and QR-based certificate generation for data integrity.
- **Forensics & Verification:** Employs advanced techniques like Entropy analysis and signature detection, fully aligned with NIST 800-88 concepts for verifiable data cleansing and migration.
- **Cloud & Storage Integration:** Features an API-abstracted secure vault layer, ensuring compatibility with major storage solutions (e.g., AWS S3, private cloud, or enterprise servers).
- **Standards Adherence:** Compliant with key industry and regulatory standards, specifically referencing NIST 800-88, ISO 27001, and the DPDP Act 2023.

III. Submission Details

Submitter Name	Team Members
Sarvesh Patil	Sai Prakash Katkade, Kaivalya Patil, Avani Atram