VIT Vellore Institute of Technology	**Invention Disclosure Format (IDF)-B**	Document No.	
		Issue No/Date	
		Amd. No/Date	0/00.00.0000

1. Title of the invention:
GuardianAI: Integrated System for AI-Driven Threat Detection and Blockchain-Based Evidence Preservation

2. Field /Area of invention:
Blockchain & AI/ML

3. Prior Patents and Publications from literature

Patent/Publications	**Title**	**Key Features**	**Limitations**
Publication	SafeGuardHer: Blockchain and Ensemble Learning based CPS Framework for Women's Safety Using Wearable Devices *-Akshat Vaja, Aarchi Dholakia, Man Patel, Keyaba Gohil, Rajesh Gupta, Sudeep Tanwar, N. Z Jhanji*	Uses bracelets and earrings with sensors to continuously monitor physiological factors. It employs Light Gradient Boosting Machine (LightGBM) as the learning model, achieving high accuracy at 94%, precision at 91.5%, and recall at 95.6%. It detects changes in physiological signals that indicate stress, providing timely warnings about potential threats. Blockchain technology is used for secure and unchangeable storage of user data and incident logs. This system combines physical wearable devices with computing power and secure communication. It is designed to work in different environments, broadly improving women's personal safety.	System effectiveness depends on users regularly wearing and maintaining the devices. Wearable devices may have limits like battery life, processing power, and connectivity issues that affect continuous monitoring. Blockchain's complexity may cause delays and scalability problems, particularly for real-time applications. Stress and threat patterns can differ from person to person, which may require retraining or adjusting the model to keep it accurate. The chance of incorrect stress detection can lead to false alarms or missed incidents, which affects reliability.
Publication	Mobile Apps for Personal Safety of Women Using Blockchain Technology- *Geeta N. Brijwani , Prafulla E. Ajmire, Varkha Jewani , and Suhashini Chaurasia*	Uses mobile applications and blockchain technology to improve security, transparency, and accountability for women's safety. Blockchain ensures secure, decentralized, and clear recording of safety-related incidents, which supports legal use and responsibility. Tackles the global and widespread challenges of women's safety across different demographics and environments.	Effectiveness depends on user adoption and consistent use of mobile devices and apps. There are potential privacy concerns about collecting and storing sensitive personal and location data. Blockchain's complexity may cause delays and scalability problems, particularly for real-time applications. The digital divide may restrict access for women in underserved or rural areas without smartphones or internet access. Challenges continue in creating widespread awareness and trust in technology-driven safety solutions.
Publication	Secure Women's Safety Platform Using Ethereum Blockchain- *By Parul*	Highlights the evolution of wearable devices from basic fitness trackers to AI-enabled	Reliance on wearables requires users to consistently adopt them and keep the

	Dubey, Pushpa Birha, *Rahul Vinayak Bambodkar*	safety tools. Integrates AI for real-time hazard evaluation and uses adaptive learning to improve situational awareness and threat detection. Uses Internet of Things (IoT) sensors, including GPS for precise location tracking and physiological monitoring for thorough safety analysis. Relies on cloud computing to provide continuous connectivity, perform computing tasks, and synchronize data across devices effectively. Supports AI-driven communication and emergency response features for immediate user assistance. Addresses ethical and privacy concerns by emphasizing strong security measures and clear data policies.	devices maintained. There are potential privacy risks linked to collecting sensitive physiological and location data. Dependence on the cloud can lead to latency, connectivity issues, and challenges with data synchronization. Energy constraints in wearables might limit their ability to monitor continuously. Ethical challenges and the need for regulatory compliance concerning data security and user consent remain important obstacles.

Prior Art (Patent/Publication)	**Key Contribution**	**Limitations Overcome by SimpliTag**
Blockchain-based method of providing secure processing of camera video	Introduces a blockchain-based security method for images taken with cameras, ensuring secure storage and preventing unauthorized access or forgery. Uses AES encryption keys to scramble image blocks and improve data privacy. Employs a blockchain to store encrypted metadata, such as keys, hash codes, and access information, without including the actual images. This reduces data load and allows for regular blockchain updates. Offers a secure image retrieval process where only authorized devices with the correct private keys can decrypt and display images. Includes hash verification to check the integrity of decrypted images, ensuring they are not forged or corrupted. Designed for use with IP cameras, CCTV, or webcams connected to networks like homes. Supports scalable blockchain updates and access from multiple devices through regular synchronization of block data and encrypted keys.	Frequent updates and encryption cause delays, limiting near real-time video access. SimpliTag uses ultra-fast consensus and lightweight blockchain designs to reduce update latency. Storing encrypted video blocks and metadata off-chain requires secure storage and management. SimpliTag improves off-chain encrypted storage with tamper-proof blockchain indexing. Multiple segment-specific encryption keys require secure distribution, renewal, and revocation among authorized users. SimpliTag offers automated key lifecycle management. Large-scale multisite deployments and frequent updates can strain blockchain networks and image processing systems. SimpliTag supports horizontally scalable, distributed architectures that are optimized for high-volume video streams and metadata sync with minimal congestion. Latency from blockchain synchronization delays the availability of the latest encrypted images. SimpliTag integrates edge computing and dynamic update intervals to enable near-real-time retrieval with strong security.
Abnormal sound monitoring system and abnormal sound monitoring method	Collects sound data inside buildings using a network of microphones. Identifies abnormal sounds by comparing collected sound features to known abnormal sound patterns. Localizes sound sources by estimating their position, the number of people involved, and direction of movement.	Installation and maintenance of multiple microphones and cameras increase system complexity and cost. SimpliTag's AI-driven sensor fusion reduces hardware needs. Accurate sound source localization is difficult in noisy or complicated indoor environments. SimpliTag uses edge computing and adaptive algorithms for

	Calculates risk values based on extracted abnormal sound information combined with source localization data. Uses a two-level risk value calculation: basic risk values linked to sound types and correction values. Integrates cameras that capture images at the sound source location for visual confirmation. Provides real-time alerts and visual risk overlays on monitoring screens for security personnel. Tracks the progression of risk values over time to assess ongoing or developing abnormal events.	noise-resilient, precise localization. Processing and communication delays between detection, risk calculation, and alerting affect responsiveness. SimpliTag uses edge computing to reduce latency and enable near real-time processing. Risk models based on predefined tables may not quickly adapt to new threats. SimpliTag includes AI-driven dynamic risk assessment that adjusts to changing contexts and new anomaly patterns. Reliance on continuous network connectivity for synchronization can lead to performance gaps. SimpliTag's distributed setup allows for offline processing and smooth synchronization.
Crime prevention system	Introduces a crime prevention system that uses an installed terminal unit, a server, and portable terminals to monitor doors or entrances. It recognizes individuals approaching the door by analyzing their face, body shape, and behavior for identification and threat assessment. It uses facial recognition with deep learning neural networks to extract and match facial features, including infrared and low-resolution images. It implements body shape recognition, classifying individuals into different body types using transfer learning on a VGG16 network for high accuracy. It incorporates voice recognition and natural language processing. It uses gyro and distance sensors to analyze movement and behavior for early detection of suspicious actions. It predicts criminal behavior by recognizing specific suspect actions. This uses behavior interpretation models built on ResNet 3D and CNN. It generates 3D facial and body modeling images for better identification and visual verification. It provides real-time alerts to users through portable terminals and can notify law enforcement or security agencies for a quick response. It supports an external image database and institutional databases. It includes vibration and side detection sensors.	The system relies on multiple sensors and components, increasing installation complexity and cost. SimpliTag's AI-enhanced sensor fusion technology reduces hardware needs. Processing large volumes of video, audio, and sensor data may cause delays and require significant computing power. SimpliTag's edge computing and optimized data processing lower latency and reduce server load. Maintaining and updating complex deep learning models for face, body, voice, and behavior recognition can require constant retraining. SimpliTag offers modular AI model management for easy updates. Securely managing user data, including biometric and behavior information, presents privacy and compliance challenges. SimpliTag provides encrypted, privacy-compliant data handling with tamper-proof blockchain-backed audit trails. Real-time notifications and communication between installed terminals, portable devices, and institutions depend on network stability. SimpliTag's distributed, scalable network infrastructure ensures strong synchronization. Cross-referencing external databases and managing various data sources can result in data integration and consistency challenges. SimpliTag's unified data framework enables smooth integration.

4. Summary and background of the invention (Address the gap / Novelty):

GuardianAI offers a major improvement in personal safety by using AI-powered multimodal threat detection and blockchain-based evidence certification. Unlike traditional safety solutions that depend on manual reporting or basic motion detection, GuardianAI constantly monitors audio and visual streams to spot distress signals like screams, threats, and dangerous gestures. It uses advanced AI models for real-time analysis, turning environmental data into feature vectors and accurately classifying situations. A standout feature of GuardianAI is how it combines threat detection with secure, unchangeable evidence storage. All audio-visual data related to incidents is timestamped and recorded on the Polygon blockchain, which creates tamper-proof records that are legally acceptable. The system is user-friendly, featuring a mobile app that automatically samples and analyzes audio with just one button press, providing instant alerts and preserving vital evidence. The innovation of GuardianAI lies in its comprehensive approach. It acts not only as a real-time safety monitor but also as a reliable "digital witness," linking fast incident response with trustworthy evidence preservation. It can be used for personal protection, like for students and commuters, as well as for occupational safety in healthcare and security roles in high-risk areas. Additionally, it offers peace of mind during ride-sharing and social events. By establishing trust through blockchain verification and objective AI, GuardianAI creates a new standard for tech-driven personal safety and legal assurance.

5. Objective(s) of Invention:

1. To improve personal safety using artificial intelligence and machine learning (AI/ML) for real-time threat detection and response.
2. To continuously monitor audio and visual data streams to spot signs of distress, aggression, or immediate danger with smart algorithms.
3. To provide users with a dependable way to capture, examine, and securely store important evidence from incidents. This builds trust and makes evidence more reliable in legal situations through tamper-proof blockchain technology.
4. The invention addresses safety gaps for individuals and organizations by delivering immediate alerts, clear analysis, and unchangeable proof for incident management and legal action.
5. By combining easy-to-use application interfaces, smooth multi-modal AI analytics, and secure storage solutions, GuardianAI wants to set new standards for real-time personal protection, workplace safety, and evidence integrity in various high-risk situations.

6. Working principle of the invent (in brief)

GuardianAI is a real-time, AI-powered personal safety monitoring system that continuously analyzes audio and visual data to spot potential threats. The system uses microphones and cameras from sources like CCTV feeds or a user's smartphone to capture ambient sounds and video streams. A simple mobile app allows users to activate a "Guard" mode, enabling live audio and location tracking for on-the-go protection. AI and machine learning algorithms process this data to identify distress signals like screams, aggressive gestures, or suspicious behaviors. When it detects unsafe conditions, the system sends immediate alerts to users and trusted contacts. At the same time, it securely stores important audio-visual evidence on a blockchain platform to ensure data integrity and legal use. This combination of proactive threat detection and tamper-proof evidence storage gives individuals better personal security and reliable documentation of incidents.

7. Description of the invention in detail (Include drawing and or photograph as needed)

Detailed Workflow of the Whole Invention:

1. Video Ingestion: A dedicated Video Ingestion Service connects directly to one or more live CCTV camera streams using the RTSP protocol.
2. Frame Processing: This service continuously pulls video frames from the CCTV feed and forwards them to the central AI Service for analysis.
3. AI Analysis (Visual): The AI Service analyzes the video for specific distress events, such as "fighting," "a person falling," or "a potential break-in."
4. Verdict Generation: If any threatening event is detected, the AI Service generates a “crime” detected classification.
5. Core API Trigger: The verdict is sent to the Core API, which acts as the central coordinator.
6. Dual-Action Trigger: The Core API initiates two actions simultaneously:
   - Alerting: It uses Twilio to send an SMS alert. The message includes the nature of the threat, the specific camera location (e.g., "Lobby Cam 1"), and a link to the location on a map.
   - Evidence Logging: It begins the blockchain notarization process with a snapshot of the critical video frames.
7. Blockchain Notarization: The Core API hashes the evidence, sends it to the Smart Contract on the Polygon blockchain, and receives a transaction hash as a receipt.
8. Confirmation & Logging: The backend saves this transaction hash to its database, creating a complete and immutable record of the incident, from detection to verification.

(The mobile app acts as a secondary, mobile trigger for the same backend system, initiating the workflow from Step 5 onwards with its audio data.)

Detailed Workflow of the Blockchain:

1. Evidence Capture: The Core API secures the critical video frames that triggered the alert from the CCTV feed.
2. Cryptographic Hashing: It uses the SHA-265 algorithm to create a unique, 64-character digital fingerprint (hash) of the video evidence.
3. Transaction Assembly: The server's wallet creates a transaction containing the hash, a timestamp, and the camera's GPS coordinates.
4. Transaction Signing: The server's private key is used to cryptographically sign the transaction, authorizing it.
5. Broadcast to Network: The signed transaction is sent to the Polygon (Amoy) network via an RPC node.
6. Smart Contract Execution: The network executes the logEvidence function on our deployed smart contract.
7. Immutable Record: The hash, timestamp, and location are permanently stored on the blockchain ledger.
8. Confirmation Receipt: The blockchain returns a unique Transaction Hash to the Core API.
9. Finalization: The Core API saves this Transaction Hash in the PostgreSQL database as permanent proof of the event.

Workflow of the App (as a mobile component):

1. Launch & Permissions: The user opens the app, which requests permissions for the microphone and location.
2. Start Guard Mode: The user presses the "START GUARD" button for personal, on-the-go monitoring.
3. Background Services: The app begins recording audio and tracking the phone's GPS location.
4. Data Submission: The app sends the recorded audio clip to the same backend server that the CCTV system uses.
5. Receiving Verdict: The app listens for a response from the server.
6. Displaying Alerts: If the server's response indicates a high-priority alert (from their own audio), the app displays a prominent on-screen Alert pop-up.

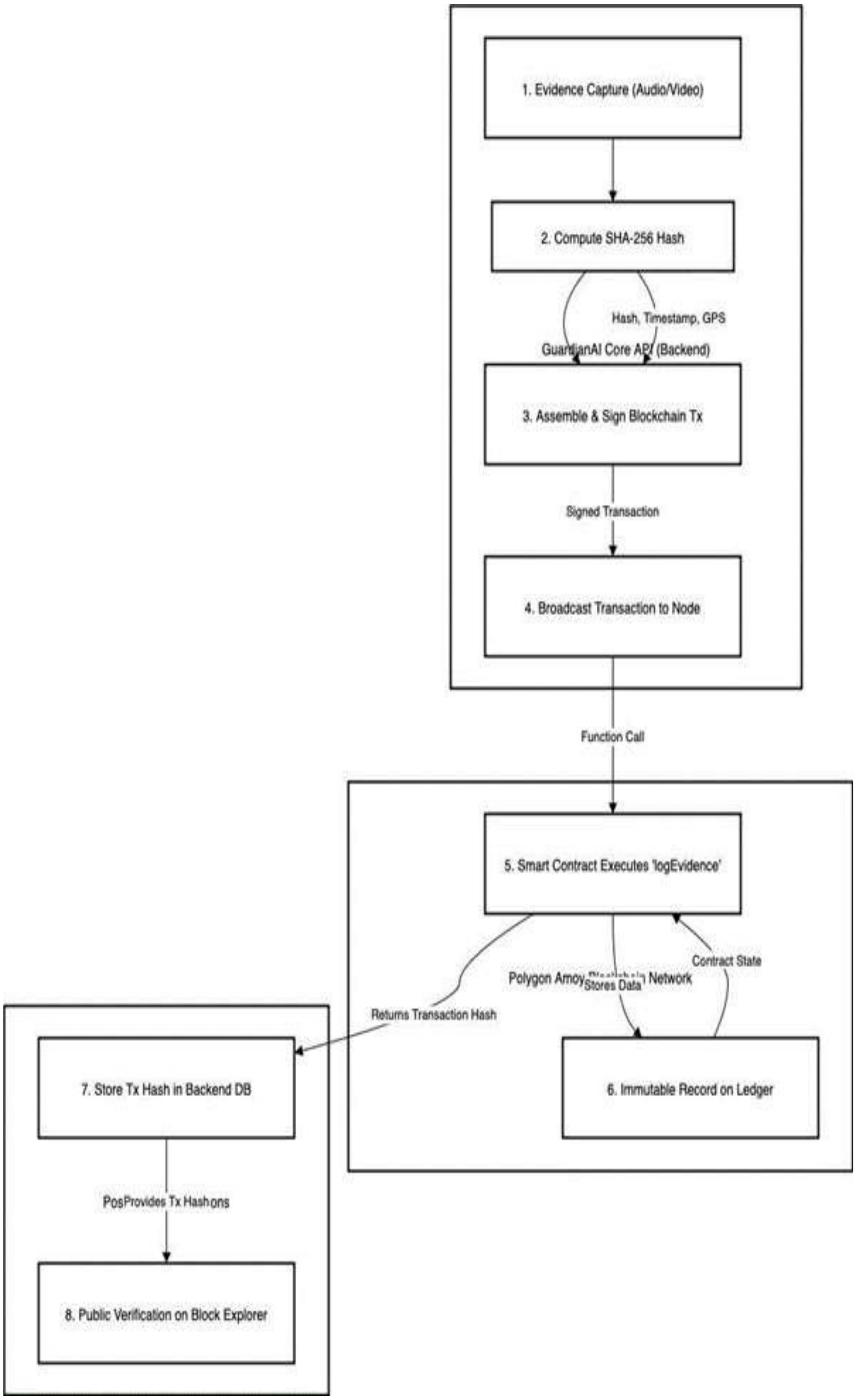
Detailed Workflow of AI Models:

1. Audio Detection Model:

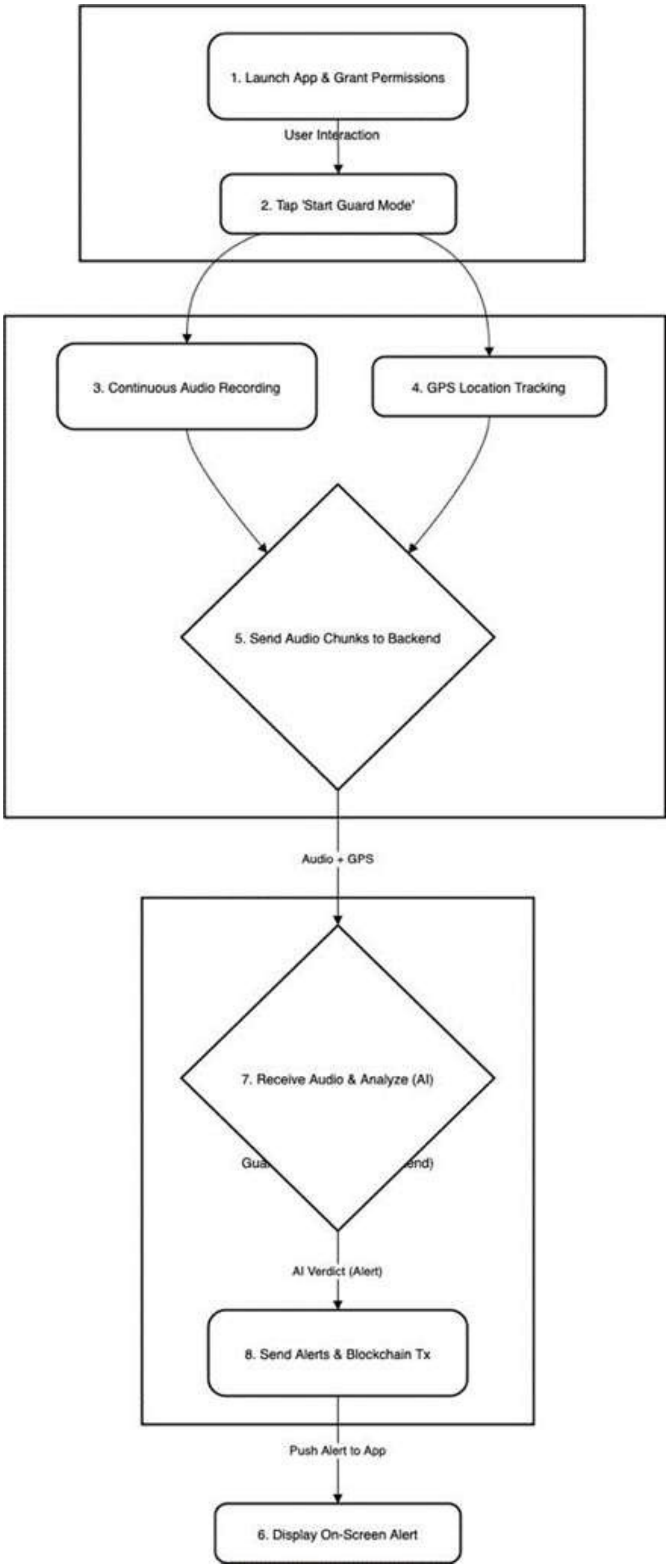
- The speech model in GuardianAI uses the pretrained model "padmalcom/wav2vec2-large-nonverbalization-classification." This model is fine-tuned to classify nonverbal vocalizations like screams, laughs, and other distress-related sounds. It is based on the wav2vec2 architecture, which is pretrained on large audio datasets, including LibriSpeech. It has also been fine-tuned on nonverbal audio collections for improved generalization.
- The model pipeline begins with audio data input. This data is loaded and processed to meet the model's sampling rate needs. The raw audio is converted into a one-dimensional waveform tensor. It is resampled if necessary and normalized.
- Next, the audio is tokenized and changed into input features using the Wav2Vec2 processor. This prepares the data for the pretrained Wav2Vec2 classification model. The model extracts deep acoustic features through self-supervised learning and performs supervised classification to identify types of vocalizations like screams or other distress signals.
- The output logits from the model become probabilities through a softmax operation, producing confidence scores for each class. If the confidence score for a critical class like "scream" is above a certain threshold, the environment is marked as unsafe.

2. Video Detection Model:

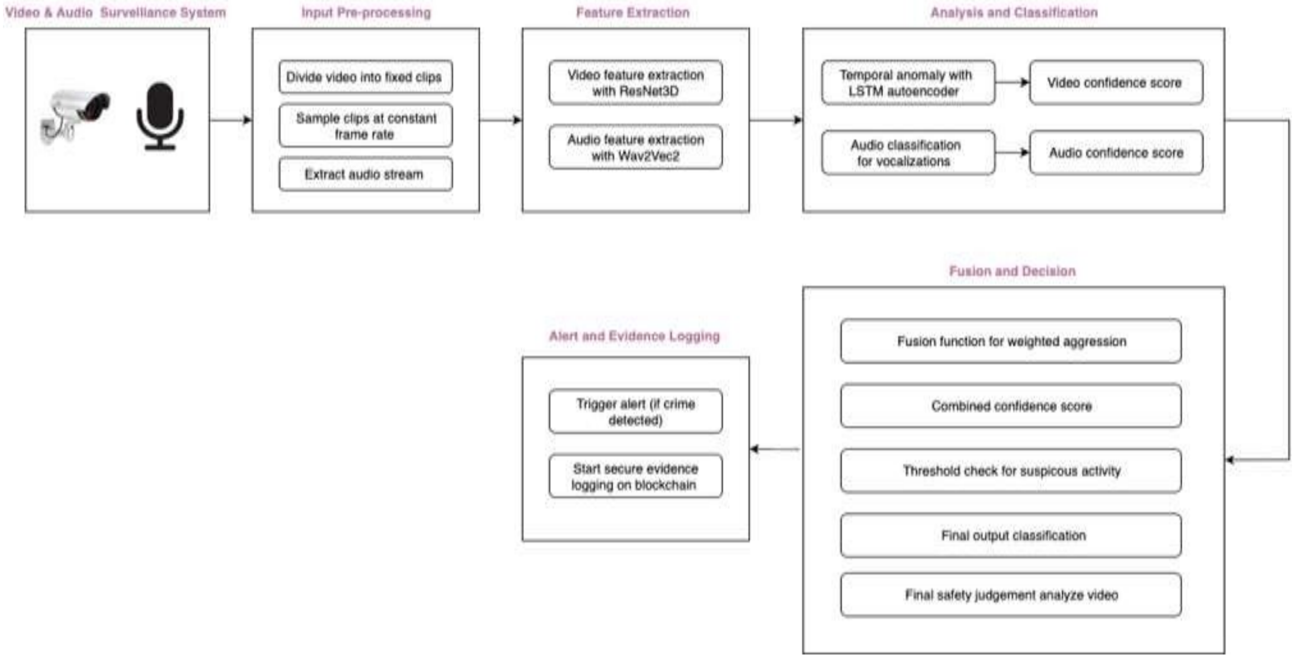
- The input video stream is divided into fixed-size clips (e.g., 16 frames), sampled at constant frame rates.
- Each clip goes through a 3D convolutional network (ResNet3D, e.g., R3D-18) that extracts spatiotemporal features, capturing appearance and motion cues.
- At the same time, audio data is processed using a pretrained speech model (e.g., Wav2Vec2), which extracts acoustic features and classifies vocalizations (e.g., screams).
- Video features are further examined by an LSTM-autoencoder to model temporal dependencies and detect anomalies based on reconstruction loss.
- The outputs from audio and video classifications produce confidence scores for categories like "crime" or "no crime."
- These scores are combined in a fusion function that applies weighted aggregation for a complete understanding of the scene and informed decision-making.
- If the combined confidence exceeds a set threshold indicating suspicious activity, the pipeline outputs "crime detected."
- Otherwise, it categorizes the environment as "no crime."
- The final analyze_video function in the GuardianAI pipeline plays an essential role in bringing together the outputs from various model components to provide a clear judgement on safety.
- Confirmed crime detections trigger alerts and start secure logging of related multimedia evidence on a blockchain to ensure tamper-proof documentation.
- This multi-model pipeline ensures reliable real-time crime classification by using complementary audio-visual cues and effective temporal modeling within an integrated decision framework.


1. Evidence Capture (Audio/Video)
2. Compute SHA-256 Hash
Hash, Timestamp, GPS
GuardianAI Core API (Backend)
3. Assemble & Sign Blockchain Tx
Signed Transaction
4. Broadcast Transaction to Node
Function Call
5. Smart Contract Executes 'logEvidence'
Contract State
Polygon Amoy Blockchain Network
Stores Data
Returns Transaction Hash
6. Immutable Record on Ledger
7. Store Tx Hash in Backend DB
PosProvides Tx Hashons
8. Public Verification on Block Explorer

App Architecture:

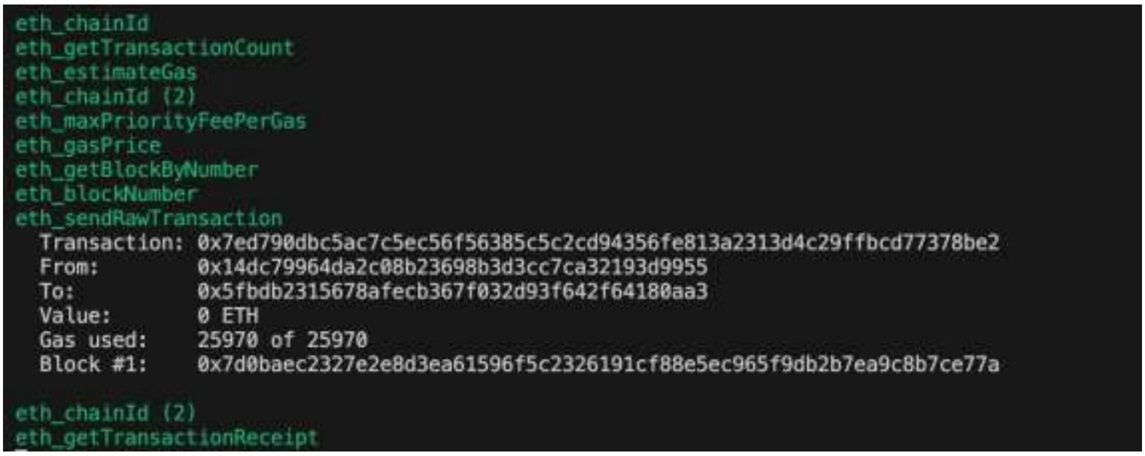

1. Launch App & Grant Permissions
User Interaction
2. Tap 'Start Guard Mode'
3. Continuous Audio Recording
4. GPS Location Tracking
5. Send Audio Chunks to Backend
Audio + GPS
7. Receive Audio & Analyze (AI)
Gua
end)
AI Verdict (Alert)
8. Send Alerts & Blockchain Tx
Push Alert to App
6. Display On-Screen Alert

Proposed System Architecture:


Video & Audio Surveillance System
Input Pre-processing
Divide video into fixed clips
Sample clips at constant frame rate
Extract audio stream
Feature Extraction
Video feature extraction with ResNet3D
Audio feature extraction with Wav2Vec2
Analysis and Classification
Temporal anomaly with LSTM autoencoder
Video confidence score
Audio classification for vocalizations
Audio confidence score
Fusion and Decision
Fusion function for weighted aggression
Combined confidence score
Threshold check for suspicous activity
Final output classification
Final safety judgement analyze video
Alert and Evidence Logging
Trigger alert (if crime detected)
Start secure evidence logging on blockchain

8.Experimental Validation Results

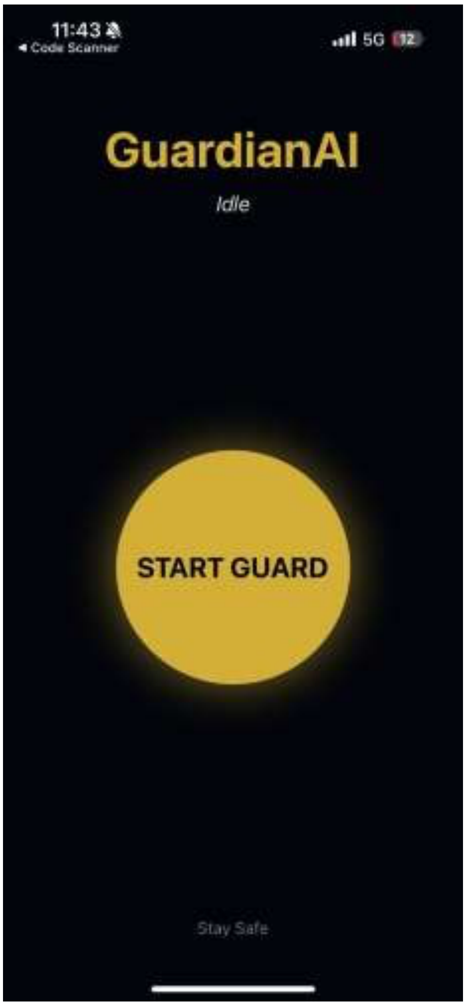
Blockchain creation:

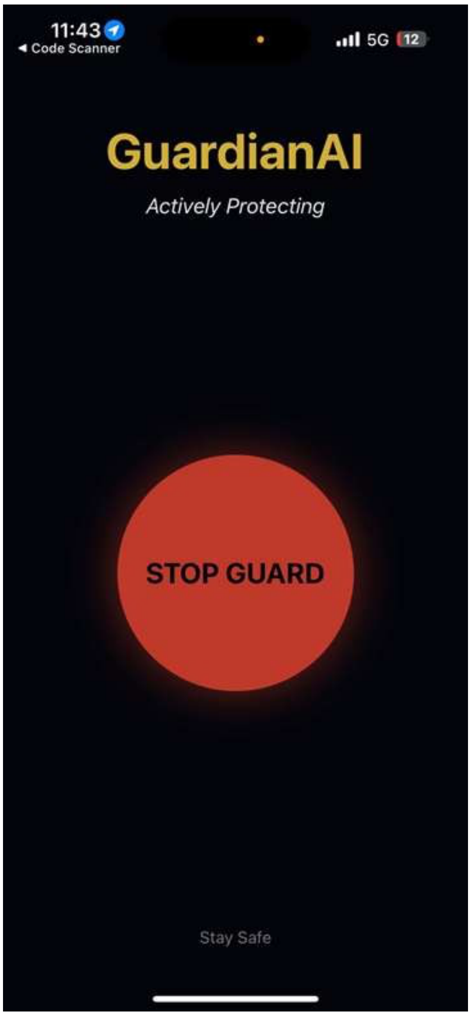


```
eth_chainId
eth_getTransactionCount
eth_estimateGas
eth_chainId (2)
eth_maxPriorityFeePerGas
eth_gasPrice
eth_getBlockByNumber
eth_blockNumber
eth_sendRawTransaction
  Transaction: 0x7ed790dbc5ac7c5ec56f56385c5c2cd94356fe813a2313d4c29ffbcd77378be2
  From:        0x14dc79964da2c08b23698b3d3cc7ca32193d9955
  To:          0x5fbdb2315678afecb367f032d93f642f64180aa3
  Value:       0 ETH
  Gas used:    25970 of 25970
  Block #1:    0x7d0baec2327e2e8d3ea61596f5c2326191cf88e5ec965f9db2b7ea9c8b7ce77a

eth_chainId (2)
eth_getTransactionReceipt
```

Mobile App interface:




11:43
◂ Code Scanner
5G
12
GuardianAI
Actively Protecting
STOP GUARD
Stay Safe

9. What aspect(s) of the invention need(s) protection?

1. A system for proactive personal safety, comprising:
   - An integrated architecture for real-time monitoring, multi-modal threat detection, incident response, and tamper-proof evidence management,
   - A user-facing application configured to access said architecture.
2. The system of claim 1, wherein the threat detection comprises:
   - A video and audio processing pipeline employing spatial-temporal feature extraction, supervised and unsupervised learning modules, fusion logic, and multi-modal classification.
3. The system of claim 1, further comprising:
   - Blockchain-based evidence storage configured to capture, authenticate, and preserve audio, video, and classification results in an immutable and legally admissible format.
4. The system of claim 1, wherein the user-facing application includes:
   - A "Guard" mode enabling continuous mobile audio capture, GPS tracking, and secure data streaming to the backend AI and blockchain evidence storage system.

10. What is Technology readiness level of your invention?

Research			Development			Deployment		
TRL 1	**TRL 2**	**TRL 3**	**TRL 4**	**TRL 5**	**TRL 6**	**TRL 7**	**TRL 8**	**TRL 9**
Basic Principles observed	Technology concept formulated	Experimental proof of concept	Technology validated in a lab	Technology validated in a relevant environment (industrially relevant in case of key enabling technologies)	Technology demonstrated in a relevant environment (industrially relevant in case of key enabling technologies)	System prototype demonstration in an operational environment	System complete and qualified	Actual system proven in an operational environment (competitive manufacturing in case of key enabling technologies, or in space)
		√	√					

Reply to the comments from the IPR cell –

1. Cryptographic Hashing Algorithm: The system uses the industry-standard SHA-256 algorithm to generate a unique, 64-character hash of the evidence file. This ensures the integrity of the evidence.

   Security Key Management: The system's security relies on several keys, all managed as secure environment variables on the backend server and never exposed to the client:

   Blockchain Private Key: Used to sign transactions and prove that requests to the smart contract originate from the GuardianAI system.

   Twilio API Keys (SID & Auth Token): Used to authenticate with the Twilio service for sending SMS alerts.

   Alchemy API Key: Part of the RPC URL used to gain access to the Polygon blockchain network.

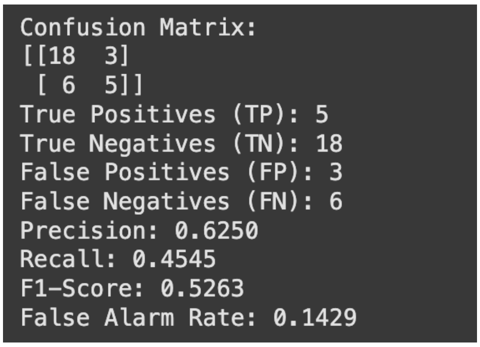
   Database Credentials: Username and password used to secure the PostgreSQL database.

2. Add datasets/metrics/latency:

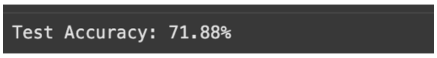
   Dataset drive link: https://www.kaggle.com/datasets/mission-ai/crimeucfdataset

   The system continuously monitors audio and visual streams. It processes this data using spatial-temporal feature extractors and multimodal classification. The metrics used include accuracy, precision, recall, and real-time detection performance for crime and distress signals. Edge computing and improved AI processing pipelines address latency. This reduces delays between detection and alerts, allowing for near real-time responsiveness.

3. Evaluate false alarms:



```
Confusion Matrix:
[[18  3]
 [ 6  5]]
True Positives (TP): 5
True Negatives (TN): 18
False Positives (FP): 3
False Negatives (FN): 6
Precision: 0.6250
Recall: 0.4545
F1-Score: 0.5263
False Alarm Rate: 0.1429
```



```
Test Accuracy: 71.88%
```

Experimental evaluation of the system demonstrates a strong overall accuracy of approximately 71.88%, reflecting effective discrimination between criminal and non-criminal video content. The total dataset is of 160 videos, split into 80:20 training and testing data (128 and 32 videos respectively). The system exhibits a balanced performance, maintaining a relatively low false alarm rate while successfully identifying a meaningful portion of anomalous events, thereby supporting reliable detection in practical scenarios. Although the current results validate the efficacy of the combined approach and its robustness across diverse video inputs, there remains clear potential for further refining sensitivity and precision, especially in accurately capturing complex or subtle criminal activities. These outcomes underscore the inventive fusion methodology’s advantage in enhancing detection accuracy while providing a foundation for continued optimization and application scalability.

4. Data Pipeline and Privacy Safeguards (DPDP/GDPR):
The system is architected with a privacy-first approach to handle sensitive data:

Data Pipeline:

Capture: The user's device or CCTV captures raw media (audio/video) and GPS data.

Transmission: Data is sent over an encrypted HTTPS channel to the Core API.

Analysis: The Core API forwards the media to the AI service, which processes it in memory and returns a JSON verdict.

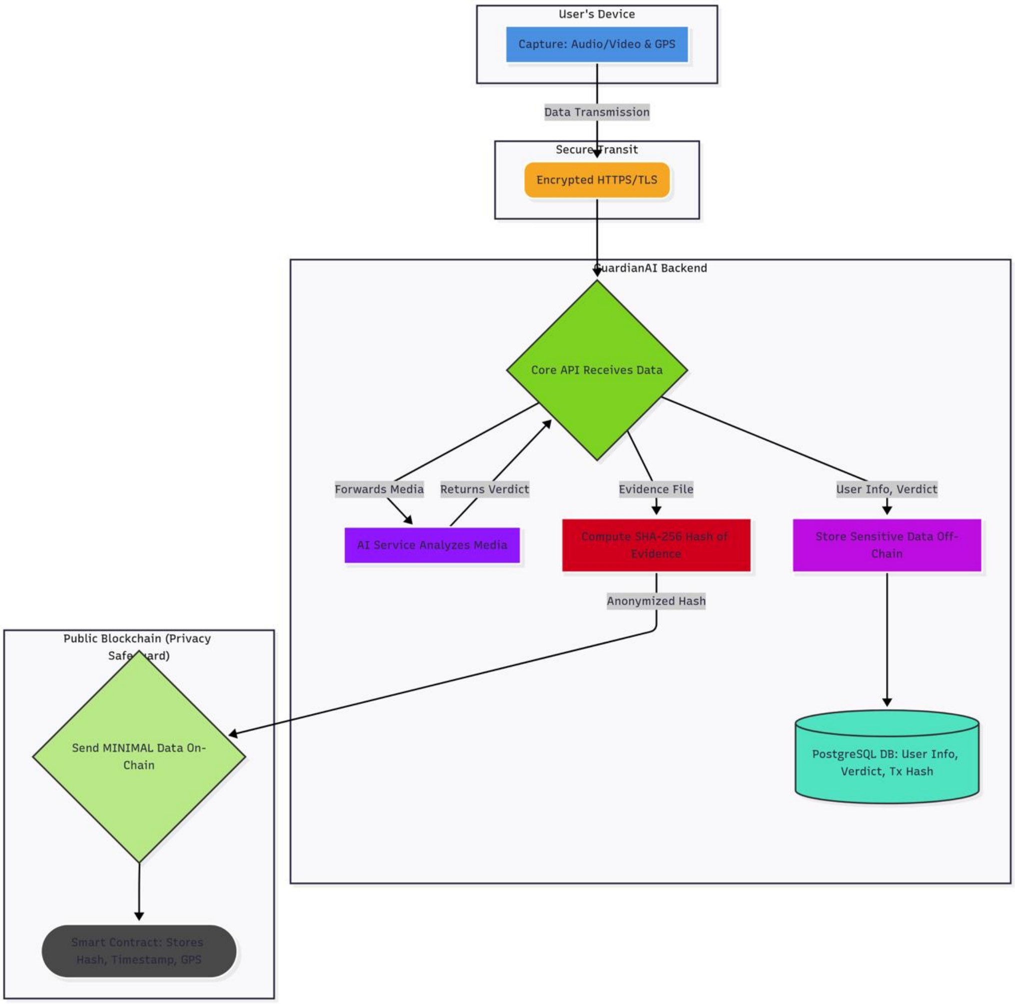
Storage: Sensitive data (user info, raw evidence files) is stored off-chain in the secure PostgreSQL database. Only an anonymized SHA-256 hash is sent to the public blockchain.

Privacy Safeguards:

Data Minimization: The most sensitive data (the raw evidence file) is never stored on the public blockchain. Only the non-personally identifiable hash is made public, complying with data minimization principles.

Encryption: All data is encrypted in transit (HTTPS). Evidence files stored off-chain are encrypted at rest.

User Consent: Monitoring only begins after the user explicitly provides consent by activating "Guard Mode" on the mobile app.


User's Device
Capture: Audio/Video & GPS
Data Transmission
Secure Transit
Encrypted HTTPS/TLS
GuardianAI Backend
Core API Receives Data
Forwards Media
Returns Verdict
Evidence File
User Info, Verdict
AI Service Analyzes Media
Compute SHA-256 Hash of Evidence
Store Sensitive Data Off-Chain
Anonymized Hash
PostgreSQL DB: User Info, Verdict, Tx Hash
Public Blockchain (Privacy Safeguard)
Send MINIMAL Data On-Chain
Smart Contract: Stores Hash, Timestamp, GPS

5. Application Binary Interface (ABI): The ABI is a JSON file generated by the Hardhat framework that acts like an API documentation for the smart contract. Our Node.js backend uses this ABI with the Ethers.js library to correctly format calls to the logEvidence function.

On-Chain vs. Off-Chain Data:

On-Chain Data: Data stored publicly on Polygon is minimal and non-sensitive: the SHA-256 hash, a timestamp, and GPS coordinates.

Off-Chain Data: All sensitive data is kept on our private backend. This includes user profiles, emergency contacts, and the raw audio/video evidence files. This hybrid approach ensures both verifiable proof and user privacy.

Blockchain Costs:

Deployment Cost: A one-time gas fee to deploy the smart contract.

Transaction Cost: A minimal gas fee (fractions of a cent) for each evidence log. We chose the Polygon network specifically for its extremely low fees, making the system economically viable.

6. Security Architecture and Operational Workflows:

Security Architecture:

Secret Management: All secrets (API keys, private keys, database passwords) are managed via secure environment variables on the server.

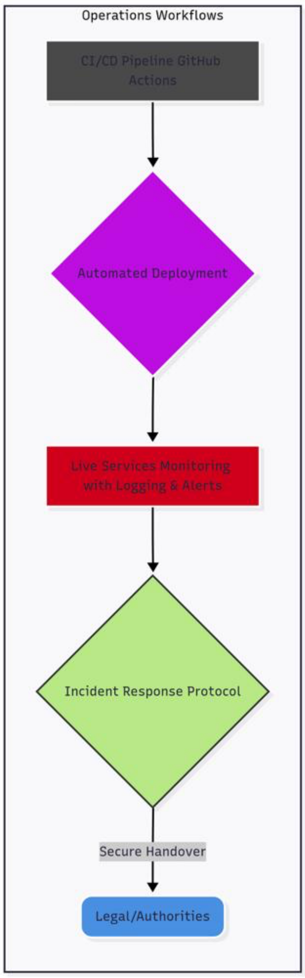
Transport Security: All communication between services is encrypted using HTTPS/TLS.

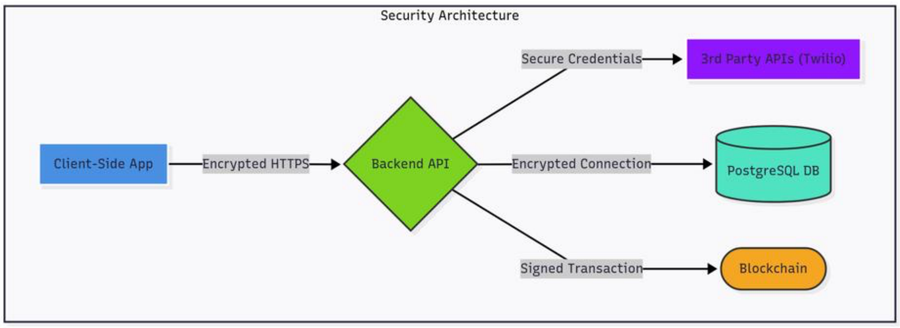
Data Integrity: SHA-256 hashing guarantees that the evidence file's integrity can be cryptographically verified against the on-chain record.

Operational Workflows:

Incident Response: When a high-priority alert is triggered, the system automatically sends alerts. An operational workflow would involve a secure procedure for providing the raw evidence file and its corresponding transaction hash to authorities upon a valid legal request.

Admin Controls: A future administrative dashboard would allow for the secure management of users and the monitoring of system health, with role-based access controls to protect sensitive data.


Operations Workflows
CI/CD Pipeline GitHub Actions
Automated Deployment
Live Services Monitoring with Logging & Alerts
Incident Response Protocol
Secure Handover
Legal/Authorities



7. Threat taxonomy and admin controls:

Threat detection includes distress signals, like screams and aggressive gestures, suspicious behaviors such as loitering and tampering, and environmental safety risks. The system uses multimodal AI classifiers trained on spatial-temporal and behavioral models, including ResNet 3D, CNN, and voice recognition. Admin controls provide role-based access, system configuration, manual override alerts, and audit features for managing incidents and ensuring compliance.