



SOFTWARE REQUIREMENTS SPECIFICATION

TrueSight : AI – Powered Spoofing Detection and Source Identification System

Date : November 14, 2025

Group Members :

Aizaz ur Rehman 2022078
Asad Ali 2022903
M. Ammaid Saleem 2022344
Hamayun Nasir 2022189

Supervisor :

Dr. M. Zain Siddiqui

Co-Supervisor :

Dr. Khurram Khan Jadoon

TrueSight : AI – Powered Spoofing Detection and Source Identification System

Revision History:

<i>Revision History</i>	<i>Date</i>	<i>Comments</i>
1.00		
2.00		

Document Approval:

The following document has been accepted and approved by the following:

<i>Signature</i>	<i>Date</i>	<i>Name</i>

List of Contents

LIST OF TABLES	4
1 INTRODUCTION	5
1.1. Problem Statement.....	5
1.2. PURPOSE	5
1.3. PRODUCT SCOPE	5
2 OVERVIEW.....	7
2.1 THE OVERALL DESCRIPTION.....	7
2.2 PRODUCT PERSPECTIVE.....	7
2.3. PRODUCT FUNCTIONS.....	7
2.4. USER CHARACTERISTICS	8
2.5. CONSTRAINTS	8
2.6. ASSUMPTIONS AND DEPENDENCIES	8
3 STATE OF THE ART	9
4 USER/SYSTEM REQUIREMENTS	10
4.1 EXTERNAL INTERFACE REQUIREMENTS.....	10
4.1.1 <i>User Interfaces</i>	10
4.1.2 <i>Hardware Interfaces</i>	10
4.1.3 <i>Software Interfaces</i>	10
4.1.4 <i>Communication Interfaces</i>	10
5 FUNCTIONAL REQUIREMENTS	11
5.1 FUNCTIONAL REQUIREMENTS WITH TRACEABILITY INFORMATION	11
6 NONFUNCTIONAL REQUIREMENTS & SOFTWARE SYSTEM ATTRIBUTES	30
6.1 PERFORMANCE REQUIREMENTS.....	31
7 PROJECT DESIGN/ARCHITECTURE	32

List of Figures

Figure 1 use cases.....	31
Figure 2 Logical View	32
Figure 3 Developmental View.....	32
Figure 4 Process View.....	32
Figure 5 Physical View	33
Figure 6 State Time Diagram.....	33
Figure 7 ER Diagram.....	33
Figure 8 Activity Diagram.....	34
Figure 9 User Interface Design	35

List of Tables

Table 1: Terms used in this document and their description.....	06
Table 2: Table for Functional Requirement 1	13
Table 3: Table for Functional Requirement 2.....	14
Table 4: Table for Functional Requirement 3	15
Table 5: Table for Functional Requirement 4.....	16
Table 6: Table for Functional Requirement 5.....	17
Table 7: Table for Functional Requirement 6.....	18
Table 8: Table for Functional Requirement 7.....	19
Table 9: Table for Functional Requirement 8.....	20
Table 10: Table for Functional Requirement 9.....	21
Table 11: Table for Functional Requirement 10.....	22
Table 12: Table for Functional Requirement 11.....	23
Table 13: Table for Functional Requirement 12.....	24
Table 14: Table for Functional Requirement 13.....	25
Table 15: Table for Functional Requirement 14.....	26
Table 16: Table for Functional Requirement 15.....	27
Table 17: Table for Functional Requirement 16.....	28
Table 17: Table for Functional Requirement 16.....	29

1 INTRODUCTION

The emergence of sophisticated deepfake technologies, fueled by generative adversarial networks (GANs), diffusion models, and voice cloning algorithms, has fundamentally escalated the vulnerability landscape for biometric authentication mechanisms. These advancements enable highly effective Presentation Attacks (PAs) across real-time digital communication platforms, including video calls, Voice over IP (VoIP), and messaging applications. Traditional unimodal authentication systems are demonstrably susceptible to dynamic deepfakes and replay attacks , necessitating the implementation of advanced multi-modal counter-measures.

The *TrueSight: AI-Powered Spoofing Detection and Source Identification System* addresses this critical security gap by proposing an AI-driven, multi-modal verification framework to ensure user authenticity and forensic traceability. The proposed system concurrently analyzes facial video, audio, and textual input streams to detect synthetic media with high precision.

1.1. Problem Statement

The rapid evolution of deepfake methodologies constitutes a dynamic attack vector compromising biometric authentication within synchronous communication channels, notably Video-over-IP. Traditional defenses are increasingly rendered obsolete by cross-modal synthesis, thereby exposing high-assurance domains such as digital banking and law enforcement to real-time identity spoofing. This vulnerability is compounded by significant deficits in forensic attribution and behavioral analytics, particularly within underrepresented linguistic landscapes like Urdu, which exacerbates regional security risks. Consequently, addressing these systemic gaps necessitates the immediate deployment of a scalable, multi-modal architecture that leverages zero-trust protocols and immutable audit trails to guarantee authentication integrity and content traceability in modern telecommunications.

1.2. Purpose

This document serves as the Software Requirements Specification (SRS) for the *TrueSight: AI-Powered Spoofing Detection and Source Identification System*. The objective is to formally delineate the verifiable functional, performance, and interface requirements that shall govern the system's design, development, and validation phases. This specification provides the foundational technical contract for the implementation team and ensures the resultant system, upon completion, satisfies the mandated security objectives and compliance guidelines, specifically aligning with international biometric standards. The primary readership includes the system development and quality assurance teams, technical management, and the final project evaluation panel.

1.3. Product Scope

The TrueSight system is defined as a dedicated, real-time, deep learning-based verification framework instantiated for the detection and mitigation of deepfake spoofing attacks in live communication services. The core scope mandates the integration of:

- **Multi-Modal Analysis:** Utilizing CNNs for lip-sync desynchronization detection and facial liveness detection using pseudo-depth supervision.
- **Linguistic Specialization:** Incorporating Urdu-specific audio processing and prosodic voice analysis for verification in multilingual contexts.
- **Forensic Source Attribution:** Implementing a module to analyze metadata (e.g., EXIF data, sensor noise), compression artifacts, generative model fingerprints, and user behavioral cues.
- **Cybersecurity Enhancements:** Integrating AI-driven anomaly detection, Multi-Factor Authentication (MFA) using behavioral biometrics, and a zero-trust security architecture.

TrueSight : AI – Powered Spoofing Detection and Source Identification System

- **Digital Forensics Traceability:** Ensuring accountability via blockchain-based tamper-proof logging and digital watermarking.

The system is delivered with a web-based interface for real-time monitoring and evidence logging. The final construct is explicitly designed to be modular, scalable, and adaptable to evolving deepfake generation techniques.

Name	Description
Deepfake	Synthetic media generated using generative AI models (e.g., GANs, diffusion models) to create highly realistic and manipulative audio, video, or text content.
Presentation Attack (PA)	An attempt to subvert a biometric verification system by presenting a counterfeit or synthetically manipulated artifact (e.g., deepfake video or cloned voice) to impersonate a legitimate user.
Multi-Modal Verification	A process that integrates and analyzes simultaneous data streams from multiple sensory modalities (e.g., facial video, audio, text) to enhance system robustness and detection precision against cross-modal attacks.
Zero-Trust Architecture	A security concept based on the principle of "never trust, always verify," requiring strict identity verification for every user and device attempting to access resources on the network, regardless of location.
Behavioral Biometrics	Measurement and analysis of unique behavioral traits (e.g., keystroke dynamics, voice stress, interaction cadence) used for continuous user authentication and anomaly detection.
Forensic Attribution	The process of tracing the origin or source of manipulated content, often involving the examination of residual artifacts, embedded fingerprints, and metadata.
Metadata	Descriptive information embedded within a file or system context, such as EXIF data, timestamps, compression artifacts, or codec-specific fingerprints, used to identify anomalies or trace content source.
CNN	Convolutional Neural Networks (CNNs) used for spatial feature extraction (e.g., facial cues)
Prosodic Analysis	The study of speech features such as pitch, rhythm, stress, and intonation, utilized in this system for detecting artificial patterns indicative of AI-cloned voices.
Blockchain Logging	The use of a decentralized, immutable digital ledger (blockchain) to record authentication events, forensic evidence, and system logs, ensuring tamper-proof integrity and legal accountability.

Table 1: Terms used and their description

2 OVERVIEW

2.1. The Overall Description

The *TrueSight* system is conceptualized as an advanced, real-time, AI-driven solution designed to counter deepfake-based spoofing attacks across live communication services, encompassing video calls, VoIP platforms, and messaging systems. It mandates a multi-modal analysis approach, integrating facial video, audio, and textual input for robust user verification. Beyond simple detection, the system incorporates advanced forensic and cybersecurity protocols to ensure end-to-end data integrity, traceability, and accountability. This framework fundamentally addresses the escalating threat posed by dynamic and cross-modal deepfakes, which render existing unimodal authentication mechanisms ineffective.

2.2. Product Perspective

The *TrueSight* system functions as a **critical component** integrated within a larger ecosystem of real-time digital communication platforms. It does not operate as a standalone application but rather as a highly specialized security layer responsible for processing, analyzing, and verifying identity streams passed from the host communication service.

The system's operational scope requires strict adherence to, and interaction with, several external interfaces:

- **System Interfaces (Communication Platform):** The system must receive synchronized, real-time facial video, audio, and potentially text data streams from external VoIP or video call platforms.
- **Software Interfaces:** The system relies on underlying operating systems and specialized libraries for deep learning inference (e.g., CNNs). It also requires interfaces for logging to an external **blockchain-based ledger**.
- **User Interfaces:** A dedicated **web-based interface** is required for real-time monitoring of authentication events, configuration management, and the review/analysis of logged forensic evidence.
- **Communication Interfaces:** The system must handle high-volume, low-latency data streams characteristic of real-time communications for effective spoofing detection.

2.3. Product Functions

The core functionality of the *TrueSight* system is defined by its seven explicit project objectives, which collectively mandate a spectrum of detection, defense, and forensic capabilities:

- **Multi-Modal Verification:** The system shall execute simultaneous and synchronized analysis of facial, audio, and text input streams to prevent deepfake-based identity spoofing.
- **Deep Learning Inference:** It shall employ Convolutional Neural Networks (CNNs) for facial liveness detection, encompassing lip-sync desynchronization and analysis of irregular facial depth patterns.
- **Localized Linguistic Analysis:** The system shall incorporate Urdu-specific audio processing and multilingual voice analysis to ensure reliable detection in linguistically diverse contexts.
- **Forensic Source Attribution:** It shall implement a dedicated module for analyzing metadata (e.g., EXIF data, sensor noise, codec fingerprints) and user behavioral patterns to identify the origin of manipulated content.

TrueSight : AI – Powered Spoofing Detection and Source Identification System

- **Security Enforcement:** The system shall integrate **AI-based anomaly detection** and Multi-Factor Authentication (MFA) utilizing **behavioral biometrics** (e.g., keystroke dynamics, voice stress).
- **Zero-Trust Protocol Implementation:** A Zero-Trust security architecture shall be enforced to protect all communication pipelines.

2.4. User Characteristics

The system is designed for two primary classes of users, each possessing distinct technical profiles and operational needs:

- **End-Users (Authenticated Users):** These are individuals interacting with the underlying communication platform who are subject to verification. Their characteristic is generally non-technical, with their interaction limited to providing valid biometric input during the authentication process.
- **Technical/Operational Stakeholders (Forensic Analysts, System Administrators):**

These users require a high degree of technical expertise. They are responsible for:

- Configuration and management of the detection thresholds and security policies.
- Real-time monitoring of authentication events and anomalies via the web interface.
- Conducting post-incident digital forensic investigations and accessing the tamper-proof logs.

2.5. Constraints

The design and development of the *TrueSight* system are subject to explicit constraints arising from its high-security and real-time nature:

- **Performance Constraints:** The system must operate in **real-time**, necessitating extremely low processing latency to prevent authentication delays in live communication services.
- **Technological Constraints (Methodology):** The core detection logic is constrained to utilize deep learning paradigms, specifically incorporating CNN models.
- **Security and Architectural Constraints:** The system **shall** be implemented adhering to a **Zero-Trust security architecture** and integrate MFA protocols.
- **Standards Compliance Constraints:** The final solution must comply with relevant international biometric authentication standards, specifically the requirements for Presentation Attack Detection (e.g., **ISO/IEC DIS 30107-3:2017**).
- **Data Integrity Constraints:** Forensic logging mechanisms are constrained to ensure **tamper-proof integrity** through the use of blockchain technology.

2.6. Assumptions and Dependencies

The viability and functionality of the *TrueSight* system rely on a foundational set of assumptions regarding the operating environment and external systems:

- **Input Data Dependency:** It is assumed that the external communication platforms (VoIP/Video Call) can provide raw, synchronized, high-fidelity audio and video streams to the TrueSight core processing engine without significant pre-processing or degradation.
- **Behavioral Biometrics Dependency:** The effectiveness of behavioral biometrics (e.g., keystroke dynamics, voice stress) is dependent upon the presence of compatible sensors or input mechanisms available on the end-user device.

- **Blockchain Infrastructure Dependency:** It is assumed that a **stable and available blockchain infrastructure** will be accessible to the system for the continuous, tamper-proof logging of forensic evidence.
- **Evolving Threat Assumption:** It is assumed that while deepfake technologies will continue to evolve, the system's **modular** design and use of **AI-driven anomaly detection** will allow for scalable and adaptive updates to maintain detection efficacy.

3 STATE OF THE ART

3.1. Literature Review

Contemporary research in digital media forensics and biometric security emphasizes the critical need for advanced Presentation Attack Detection (PAD) mechanisms, largely in response to the proliferation of deepfake content generated by sophisticated deep learning models (GANs, diffusion models). The literature advocates a shift from traditional unimodal authentication methods (e.g., singular facial or voice recognition) towards a **multi-modal verification framework** for enhanced resilience against dynamic, cross-modal spoofing.

Key areas of focus, reflected in this system's design, include:

- **Livehood Detection:** Deep learning techniques, particularly CNNs with pixel-wise supervision, are explored to detect anomalies such as lip-sync mismatches, irregular facial depth, and texture artifacts.
- **Source Attribution:** The field stresses the integration of advanced digital forensic methods to examine underlying media characteristics, including metadata (EXIF, sensor noise, compression artifacts) and generative model fingerprints, to trace the content's origin.
- **Acoustic Features:** Recent work highlights the importance of prosodic voice analysis for real/fake voice classification, alongside the necessity for cross-lingual detection techniques to serve low-resource and multilingual environments.
- **Cybersecurity Integration:** The literature increasingly supports embedding robust cybersecurity enhancements such as AI-powered anomaly detection, Multi-Factor Authentication (MFA) utilizing behavioral biometrics, and implementation of a zero-trust security architecture to secure data integrity and communication pipelines.
- **Accountability and Traceability:** Mechanisms ensuring tamper-proof evidence logging, specifically referencing blockchain-based logging and digital Signature, are cited as essential for post-incident analysis and legal compliance.

3.2. Existing Systems

Analysis of existing systems reveals their principal limitations against the complexity of modern deepfake threats, providing the direct justification for the proposed **TrueSight** solution.

Existing System Category	Features & Current State	Identified Weaknesses (Gaps)	TrueSight's Response to Weaknesses
Liveness Face Detection	Employs facial motion, depth estimation, and texture analysis for static attack detection in live calls.	Critically ineffective against dynamic deepfakes . Lacks advanced metadata forensics (e.g., codec fingerprints, sensor noise). Insufficiently integrated with robust cybersecurity protocols (MFA, zero-trust).	Integrates pixel-wise pseudo depth labels and saliency maps. Implements advanced metadata analysis (EXIF, sensor noise, compression artifacts). Deploys AI-driven anomaly detection, behavioral biometrics via MFA, and a zero-trust architecture .
Voice Authentication	Uses voice biometrics, spectral analysis, and phoneme recognition. Relies minimally on metadata usage.	Highly vulnerable to AI-cloned voices . Deficient in cross-modal validation (i.e., correlating voice with lip movements). Lacks Urdu-specific detection models. Absence of advanced metadata forensics and robust cybersecurity layers.	Adds lip-sync verification and specialized Urdu-specific linguistic analysis . Incorporates prosodic analysis for precise real/fake voice classification. Integrates advanced metadata forensics and the full suite of cybersecurity protocols (MFA, behavioral biometrics, blockchain logging).

4 USER/SYSTEM REQUIREMENTS

4.1. External Interface Requirements

This subsection delineates the necessary external system, hardware, software, and communication interfaces required for the effective deployment and continuous operation of the **TrueSight** system within the context of live digital communication platforms.

4.1.1. User Interfaces

The User Interface (UI) component shall be implemented as a dedicated **web-based interface**. This interface is mandatory for operational stakeholders and must provide distinct functionalities for system observability and forensic accountability :

- **Real-Time Monitoring:** The interface shall provide continuous display and monitoring of all active authentication events.
- **Forensic Access:** It must facilitate the review and analysis of all detected anomalies and forensic evidence, utilizing the outputs from the tamper-proof logging mechanisms.
- **Configuration (Derived):** The interface must allow technical personnel to configure policies, such as Multi-Factor Authentication (MFA) parameters and detection thresholds.

4.1.2. Hardware Interfaces

The system's reliance on computationally intensive deep learning models (CNNs and RNNs) imposes specific requirements on the execution hardware:

- **High-Performance Processing:** The infrastructure must support real-time deep learning inference, specifically accommodating the simultaneous execution of multi-modal data fusion and analysis at low latency.
- **Resource Allocation:** Hardware resources must be adequate to maintain the integrity of the integrated zero-trust security architecture and manage the data throughput associated with live communication streams.

4.1.3. Software Interfaces

The *TrueSight* system is functionally dependent on programmatic interfaces with the following external software components and standards:

- **Host Communication Platforms:** Interfaces are mandatory for receiving synchronized, high-fidelity facial video, audio, and textual input streams from external VoIP or video call services.
- **Deep Learning Engines:** Interfaces must be established for seamless execution and control of the system's core deep learning modules, including CNNs.
- **Forensic Ledger Interface:** A dedicated software connection is required to facilitate the continuous, tamper-proof logging of forensic evidence onto the designated blockchain-based ledger.
- **Security & Biometrics:** Interoperability is required with modules enforcing MFA and behavioral biometrics (e.g., keystroke dynamics, voice stress analysis).

4.1.4. Communication Interfaces

The communication interfaces must be engineered to handle the technical parameters of real-time operation and high-security data transfer:

- **High-Throughput, Synchronous Data:** The interfaces must reliably manage high-volume, low-latency transmission of synchronous video and audio data streams, which are critical for temporal analysis (e.g., lip-sync detection).
- **Protocol Security:** All data transmission across the network interfaces must adhere to and be protected by the implemented zero-trust security protocols and supporting advanced cybersecurity mechanisms.

5 Functional Requirements

5.1 Functional Requirements

5.1.1 Core Detection & Analysis :

- Multi-Modal Stream Processing
- Lip-Sync Discrepancy Detection (CNN Execution)
- Facial Spoofing Cues Detection (Deep Learning Execution)
- Synthetic Audio Patterns Detection (Deep Learning Execution)
- Urdu-Specific Audio Processing
- Multilingual Voice Analysis

5.1.2 Forensic Source Identification

- Metadata Forensic Examination
- Compression Artifacts Forensic Examination
- Sensor Noise Forensic Examination
- Behavioral Patterns Analysis (Cadence/Interaction)
- Generative Model Fingerprints Forensic Attribution

5.1.3 Security, Traceability, & Infrastructure

- AI-Powered Anomaly Detection
- Tamper-Proof Logging (Blockchain Implementation)
- Forensic Watermarking Application
- Real-Time Authentication Event Monitoring (Web Interface)
- Forensic Evidence Log Review (Web Interface)
- System Functionality Adaptation (Modularity)

5.2 Functional Requirements with Traceability information

Field	Assignment Format/Value	Technical Significance
Requirement ID	FR-[Category]-[Number] (e.g., FR-DA-01)	Provides a unique identifier for Forward Traceability to design, test cases, and source code modules.
Use Case #	UC-[Number] (e.g., UC-01, UC-03)	Links the functional requirement to a specific end-user interaction or system scenario.
Parent Requirement #	O-[Number] (e.g., O-2, O-6)	Provides the Backward Traceability link to the originating high-level system objective outlined in the project scope.

5.2.1 Core Detection & Analysis :

➤ Multi-Modal Stream Processing :

The architecture must support concurrent, real-time fusion of heterogeneous data streams (video, audio, text), maintaining strict temporal synchronization. This foundational multi-modal processing service is essential for cross-modal validation to mitigate synchronized deepfake presentation attacks.

Requirement ID	FR-DA-01	Requirement Type	Functional		Use Case #	UC-01					
Status	New	Agreed-to	-	Baselined	-	Rejected	-				
Parent Requirement #	O-2										
Description	The system shall perform real-time, synchronous fusion and processing of facial video, audio, and textual input streams to execute identity verification.										
Rationale	Cross-modal analysis is the necessary countermeasure against sophisticated deepfakes that exploit the limitations of unimodal authentication systems.										
Source	System Requirements Specification (SyRS)	Source Document	-								
Acceptance/Fit Criteria	The system must successfully ingest and synchronize the three data streams (video, audio, text) within ≤ 10 ms latency and process them concurrently for a defined session duration.										
Dependencies	Requires functional Communication Interfaces and adequate Hardware Interfaces for stream throughput.										
Priority	Essential	Conditional	-	Optional	-						
Change History	Initial Draft										

Table 2: Table for Functional Requirement 1

➤ **Lip-Sync Discrepancy Detection (CNN Execution) :**

This function implements the temporal analysis component of video verification. It involves utilizing a combined Convolutional and Recurrent Neural Network (CNN) architecture to detect deviations in mouth movements that are inconsistent with the corresponding speech signal, a tell-tale sign of synthetic media generation.

Requirement ID	FR-DA-02	Requirement Type	Functional	Use Case #	UC-01							
Status	New	Agreed-to	-	Baselined	-	Rejected	-					
Parent Requirement #	O-1											
Description	The system shall employ a CNN based model to perform temporal analysis and detect lip-sync desynchronization between the video and audio streams in real-time.											
Rationale	Temporal correlation analysis is a fundamental method to defeat dynamic deepfakes where synchronization artifacts are frequently present.											
Source	AI Model Training Plan Algorithm Design Specification			Source Document	-							
Acceptance/Fit Criteria	The model must correctly flag a synthesized video with an intentionally induced lip-sync offset of ≥ 50 ms as an attack.											
Dependencies	Depends on FR-DA-01 (Stream Processing) and Software Interfaces for model execution.											
Priority	Essential	Conditional	-	Optional	-							
Change History	Initial Draft											

Table 3: Table for Functional Requirement 2

➤ **Facial Spoofing Cues Detection (Deep Learning Execution) :**

This service focuses on the spatial analysis of video frames to identify visual artifacts indicative of a fabricated identity. It employs deep learning methods, often supervised by synthetic data (e.g., pseudo-depth maps), to detect non-physical cues such as unnatural eye blinking, skin texture anomalies, or irregular facial depth patterns.

Requirement ID	FR-DA-03	Requirement Type	Functional	Use Case #	UC-01					
Status	New	Agreed-to	-	Baselined	-	Rejected	-			
Parent Requirement #	O-1									
Description	The system shall employ a Deep Learning module (CNNs) to detect subtle facial spoofing cues, including texture artifacts and irregular facial depth patterns, using techniques like pixel-wise pseudo depth labels.									
Rationale	Direct defense against dynamic presentation attacks by enforcing visual liveness and physical consistency.									
Source	ISO/IEC DIS 30107-3 (PAD Criteria) Algorithm Design Specification			Source Document	-					
Acceptance/Fit Criteria	The module must maintain an Attack Presentation Classification Error Rate (APCER) below 5% against known deepfake datasets.									
Dependencies	Depends on FR-DA-01 (Stream Processing) and robust Hardware Interfaces for high-resolution analysis.									
Priority	Essential	Conditional	-	Optional	-					
Change History	Initial Draft									

Table 4: Table for Functional Requirement 3

➤ **Synthetic Audio Patterns Detection (Deep Learning Execution) :**

This requirement addresses the detection of purely fabricated or cloned voice tracks. It necessitates the use of deep learning and specialized audio processing to identify artificiality, often focusing on acoustic features and micro-irregularities that deviate from natural human speech patterns.

Requirement ID	FR-DA-04	Requirement Type	Functional	Use Case #	UC-01					
Status	New	Agreed-to	-	Baselined	-	Rejected	-			
Parent Requirement #	O-1									
Description	The system shall employ Deep Learning models for the real-time detection and classification of synthetic audio patterns indicative of AI-cloned voices									
Rationale	Essential to neutralize voice cloning, a primary vector for impersonation attacks in VoIP and messaging platforms.									
Source	Voice Biometrics Standard (e.g., ISO/IEC 19794) Acoustic Feature Specification			Source Document	-					
Acceptance/Fit Criteria	The audio detection component must achieve a False Rejection Rate (FRR) of $\leq 3\%$ against legitimate user voices.									
Dependencies	Depends on FR-DA-01 (Stream Processing) and access to a comprehensive database of known voice samples/cloning artifacts.									
Priority	Essential	Conditional	-	Optional	-					
Change History	Initial Draft									

Table 5: Table for Functional Requirement 4

➤ **Urdu-Specific Audio Processing :**

Addressing the stated vulnerability in local linguistic contexts, this function demands the incorporation of specialized language processing modules. These modules must be optimized for the acoustic and prosodic features unique to the Urdu language, enhancing detection accuracy where generalized models fail due to resource limitations.

Requirement ID	FR-DA-05	Requirement Type	Functional	Use Case #	UC-01					
Status	New	Agreed-to	-	Baselined	-	Rejected	-			
Parent Requirement #	O-3									
Description	The system shall incorporate dedicated modules to perform Urdu-specific audio processing and acoustic feature extraction to validate speech authenticity.									
Rationale	Mandatory due to the critical gap and increased vulnerability of current systems in multilingual contexts like Pakistan.									
Source	Linguistic Research Paper (Urdu Prosody) Localized Training Data Specification			Source Document	-					
Acceptance/Fit Criteria	The Urdu detection model must demonstrate a measurable improvement (e.g., $\geq 10\%$ increase in F1 score) over generic detection models when tested on Urdu deepfake corpora.									
Dependencies	Requires FR-DA-04 (Synthetic Audio Detection) and the Multilingual Voice Analysis (FR-DA-06) module.									
Priority	Essential	Conditional	-	Optional	-					
Change History	Initial Draft									

Table 6: Table for Functional Requirement 5

➤ **Multilingual Voice Analysis :**

Extending beyond the primary Urdu focus, this function ensures the system's broad applicability. It requires the ability to analyze and categorize voice features (prosody, cadence) across multiple linguistic profiles, preventing non-Urdu language spoofing attacks.

Requirement ID	FR-DA-06	Requirement Type		Functional	Use Case #		UC-01			
Status	New	Agreed-to	-	Baselined	-	Rejected	-			
Parent Requirement #	O-3									
Description	The system shall perform generalized multilingual voice analysis, including prosodic analysis, to improve detection accuracy across diverse linguistic inputs.									
Rationale	Ensures the solution is resilient and scalable for use beyond the primary target language, fulfilling O-3's objective for "other multilingual contexts".									
Source	Prosodic Feature Extraction Documentation Speech Analysis Library API Specification			Source Document	-					
Acceptance/Fit Criteria	The multilingual module must process and return a detection confidence score for at least three major global languages beyond Urdu.									
Dependencies	Depends on FR-DA-04 (Synthetic Audio Detection) and requires a curated multilingual audio corpus.									
Priority	Essential	Conditional	-	Optional	-					
Change History	Initial Draft									

Table 7: Table for Functional Requirement 6

5.2.2 Forensic Source Identification

➤ Metadata Forensic Examination :

This requirement is foundational to the "Source Identification" component. It demands the deep inspection of file and stream metadata (e.g., EXIF data, timestamps) associated with the input stream to uncover inconsistencies or forensic signatures that indicate manipulation, prior processing, or tampering.

Requirement ID	FR-FI-01	Requirement Type		Functional		Use Case #	UC-02			
Status	New		Agreed-to	-	Baselined	-	Rejected			
Parent Requirement #	O-4									
Description	The system shall execute advanced digital forensic techniques to examine and validate stream metadata, including EXIF data and timestamps, for signs of tampering or reprocessing.									
Rationale	Metadata integrity checking is vital for source tracing and accountability, moving beyond simple detection									
Source	Digital Media Forensic Standards (e.g., NIST SP 800-86) Input Stream Specification			Source Document	-					
Acceptance/Fit Criteria	The module must successfully parse and analyze at least four distinct metadata types (e.g., EXIF, timestamp, file size, codec ID) from the incoming streams.									
Dependencies	Requires stable Software Interfaces to access metadata libraries.									
Priority	Essential		Conditional	-	Optional	-				
Change History	Initial Draft									

Table 8: Table for Functional Requirement 7

➤ **Compression Artifacts Forensic Examination :**

This function utilizes the fact that media manipulation introduces specific digital artifacts when re-compressed. The system must analyze compression-related noise, blocking, and color degradation, specifically those related to codec fingerprints, to detect instances where media has been repeatedly processed or synthesized

Requirement ID	FR-FI-02	Requirement Type	Functional	Use Case #	UC-02			
Status	New	Agreed-to	-	Baselined	-	Rejected	-	
Parent Requirement #	O-4							
Description	The system shall analyze multimedia streams for irregularities in compression artifacts and codec-specific fingerprints characteristic of re-encoding or synthetic manipulation.							
Rationale	Compression artifact analysis is a standard digital forensic technique used to identify manipulated content that has undergone multiple compression cycles.							
Source	JPEG/MPEG Codec Specification Digital Forensics Tool Documentation	Source Document	-					
Acceptance/Fit Criteria	The module must identify three specific indicators of recompression (e.g., blockiness, color bleeding, high frequency loss) in a test file known to be re-encoded.							
Dependencies	Requires direct access to the raw media streams before host platform re-encoding.							
Priority	Essential	Conditional	-	Optional	-			
Change History	Initial Draft							

Table 9: Table for Functional Requirement 8

➤ **Sensor Noise Forensic Examination :**

This advanced technique focuses on identifying intrinsic hardware signatures. The system must analyze minute noise patterns (often Photo-Response Non-Uniformity or PRNU) present in video frames to determine if the stream originated from the claimed camera sensor or if it was inserted digitally from a distinct source.

Requirement ID	FR-FI-03	Requirement Type	Functional	Use Case #	UC-02					
Status	New	Agreed-to	-	Baselined	-	Rejected	-			
Parent Requirement #	O-4									
Description	The system shall analyze video frames for abnormal sensor noise patterns to detect evidence of digital stream insertion not originating from a physical camera sensor.									
Rationale	Sensor noise analysis provides a unique hardware-based fingerprint for source identification, addressing one aspect of forensic source detection									
Source	PRNU (Photo-Response Non-Uniformity) Research Papers Hardware Sensor Specification			Source Document	-					
Acceptance/Fit Criteria	The module must successfully distinguish between a video captured from a genuine camera and a digitally rendered/replayed video lacking characteristic sensor noise patterns.									
Dependencies	Highly dependent on the quality of the input stream provided by the Communication Interfaces									
Priority	Essential	Conditional	-	Optional	-					
Change History	Initial Draft									

Table 10: Table for Functional Requirement 9

➤ Behavioral Patterns Analysis (Cadence/Interaction) :

This is a behavioral biometric function that analyzes the natural rhythm and timing of user interaction, specifically focusing on speech cadence and overall interaction irregularities. Deepfakes may perfectly replicate voice pitch but fail to capture human timing and interaction dynamics.

Requirement ID	FR-FI-04	Requirement Type	Functional	Use Case #	UC-02							
Status	New	Agreed-to	-	Baselined	-	Rejected	-					
Parent Requirement #	O-4											
Description	The system shall analyze speech cadence irregularities and interaction anomalies as a component of the behavioral analysis for source tracing and impersonation detection.											
Rationale	Provides an effective non-technical defense mechanism against synthetic media that fails to emulate human interaction timing and dynamics.											
Source	Behavioral Biometrics Protocol Specification Cognitive Psychology Research			Source Document	-							
Acceptance/Fit Criteria	The module must establish a baseline user speech cadence profile and flag deviations of $\geq 20\%$ in pause duration or response time as anomalous.											
Dependencies	Requires consistent user baseline data and FR-DA-06 (Multilingual Voice Analysis) for prosodic input.											
Priority	Essential	Conditional	-	Optional	-							
Change History	Initial Draft											

Table 11: Table for Functional Requirement 10

➤ **Generative Model Fingerprints Forensic Attribution :**

This is a high-level forensic function that attempts to identify the source software. It leverages specific, subtle patterns left by the Generative Adversarial Networks (GANs) or diffusion models used to create the deepfake, acting as a "signature" of the synthesis tool.

Requirement ID	FR-FI-05		Requirement Type		Functional		Use Case #		UC-02						
Status	New	Agreed-to	-	Baselined	-	Rejected	-								
Parent Requirement #	O-4														
Description	The system shall incorporate techniques for the forensic attribution of content based on detecting and identifying generative model fingerprints left by AI synthesis tools														
Rationale	Essential for full source tracing, identifying not just the manipulation but the class of tool used, supporting legal accountability.														
Source	AI Source Attribution Research GAN/Diffusion Model Artifacts Library			Source Document		-									
Acceptance/Fit Criteria	The attribution module must correctly classify the generative model family (e.g., GAN or Diffusion) in $\geq 75\%$ of test cases against a curated deepfake database.														
Dependencies	Requires FR-FI-03 (Sensor Noise Analysis) as a complementary technique.														
Priority	Essential	Conditional	-	Optional	-										
Change History	Initial Draft														

Table 12: Table for Functional Requirement 11

5.2.3 Security, Traceability, & Infrastructure

➤ **AI-Powered Anomaly Detection :**

This service focuses on monitoring the system's runtime environment for suspicious access patterns, processing anomalies, or unusual resource consumption that could signify an internal breach or a novel attack vector not covered by the core detection models.

Requirement ID	FR-ST-01	Requirement Type		Functional	Use Case #		UC-04					
Status	New	Agreed-to	-	Baselined	-	Rejected	-					
Parent Requirement #	O-5											
Description	The system shall employ AI-based anomaly detection to monitor session states and system logs for unexpected operational patterns indicative of a security threat.											
Rationale	Provides a dynamic, adaptive layer of defense against unknown or zero-day security threats											
Source	Security Monitoring Policy Document SIEM System Architecture			Source Document	-							
Acceptance/Fit Criteria	The module must maintain a False Positive Rate (FPR) of session flagging at $\leq 0.5\%$.											
Dependencies	Depends on FR-ST-06 (Real-Time Monitoring) and log aggregation capabilities.											
Priority	Essential	Conditional	-	Optional	-							
Change History	Initial Draft											

Table 13: Table for Functional Requirement 12

➤ **Tamper-Proof Logging (Blockchain Implementation) :**

This function establishes the immutability of forensic evidence. The system must interact with an external blockchain infrastructure to commit all evidence records, guaranteeing that once logged, the data cannot be altered or repudiated.

Requirement ID	FR-ST-04	Requirement Type		Functional	Use Case #		UC-03			
Status	New	Agreed-to	-	Baselined	-	Rejected	-			
Parent Requirement #	O-6									
Description	The system shall utilize a blockchain-based logging mechanism to record all authentication events and forensic evidence, ensuring tamper-proof integrity and traceability.									
Rationale	Ensures evidence integrity for compliance and legal accountability, addressing the weakness of unsecured logging.									
Source	Blockchain Ledger Technical Specification Cryptographic Hashing Protocol Document			Source Document	-					
Acceptance/Fit Criteria	All forensic evidence packets must be successfully hashed and committed to the blockchain, yielding a verifiable transaction ID, with latency ≤ 2 seconds.									
Dependencies	Requires reliable access to a blockchain infrastructure and the Forensic Watermarking Application (FR-ST-05).									
Priority	Essential	Conditional	-	Optional	-					
Change History	Initial Draft									

Table 14: Table for Functional Requirement 13

➤ **Forensic Watermarking Application :**

This mechanism involves embedding an unnoticeable, traceable digital watermark into the data streams or evidence packets. This watermark serves as a proprietary identifier that can later be extracted to confirm the source, integrity, and authenticity of the media or log data.

Requirement ID	FR-ST-05	Requirement Type		Functional	Use Case #		UC-03			
Status	New	Agreed-to	-	Baselined	-	Rejected	-			
Parent Requirement #	O-6									
Description	The system shall implement digital watermarking of generated forensic evidence and logs to ensure the traceability and accountability of collected data.									
Rationale	A key mechanism for accountability and ensuring the chain-of-custody for digital evidence.									
Source	Digital Watermarking Standard (e.g., ISO 17978) Media Integrity Policy			Source Document	-					
Acceptance/Fit Criteria	The watermarking process must embed a unique identifier into the evidence file without degradation of the primary content quality (perceptual quality metric ≥ 4.5).									
Dependencies	Output is linked to FR-ST-04 (Blockchain Logging).									
Priority	Essential	Conditional	-	Optional	-					
Change History	Initial Draft									

Table 15: Table for Functional Requirement 14

➤ **Real-Time Authentication Event Monitoring (Web Interface) :**

This function defines the operational visibility layer for security personnel. The web interface must continuously aggregate, filter, and display the ongoing results of the verification processes, including alerts generated by the anomaly detection module.

Requirement ID	FR-ST-06	Requirement Type		Functional	Use Case #		UC-04			
Status	New	Agreed-to	-	Baselined	-	Rejected	-			
Parent Requirement #	O-7									
Description	The system shall provide a web-based interface element dedicated to displaying live authentication decisions and system anomaly alerts in real-time.									
Rationale	Ensures operational visibility for technical stakeholders and is a mandatory component of the web-based interface delivery.									
Source	User Interface (UI) Wireframe Specification Operational Dashboard Requirements			Source Document	-					
Acceptance/Fit Criteria	The interface latency for displaying an event outcome must not exceed 1 second after the verification core makes a decision.									
Dependencies	Requires FR-ST-01 (Anomaly Detection) as a source of alerts.									
Priority	Essential	Conditional	-	Optional	-					
Change History	Initial Draft									

Table 16: Table for Functional Requirement 15

➤ **Forensic Evidence Log Review (Web Interface) :**

This is the interface function for post-incident analysis. It must allow authorized technical personnel to query, filter, and review the immutable historical records stored in the blockchain ledger, including associated forensic evidence links.

Requirement ID	FR-ST-07	Requirement Type		Functional	Use Case #		UC-03			
Status	New	Agreed-to	-	Baselined	-	Rejected	-			
Parent Requirement #	O-7									
Description	The system shall provide a web-based interface element allowing authorized personnel to query and review the tamper-proof forensic evidence and authentication logs.									
Rationale	Necessary interface functionality for digital forensic investigations and retrieving logs for legal accountability.									
Source	UI Wireframe Specification Data Retrieval and Query Language Specification			Source Document	-					
Acceptance/Fit Criteria	The search function must retrieve log records based on three filtering criteria (e.g., date, user ID, anomaly type) within ≥ 5 seconds .									
Dependencies	Requires FR-ST-04 (Blockchain Logging) as the data source.									
Priority	Essential	Conditional	-	Optional	-					
Change History	Initial Draft									

Table 17: Table for Functional Requirement 16

➤ **System Functionality Adaptation (Modularity) :**

This is an architectural requirement emphasizing modularity to ensure long-term relevance. The system must be structured into loosely coupled components, allowing individual deep learning modules or forensic techniques to be updated, replaced, or retrained without affecting the entire core framework.

Requirement ID	FR-ST-08	Requirement Type	Functional	Use Case #	UC-05					
Status	New	Agreed-to	-	Baselined	-	Rejected	-			
Parent Requirement #	O-7									
Description	The system shall be designed with a modular architecture to ensure ease of component replacement, updates, and overall functional adaptation to evolving deepfake generation techniques.									
Rationale	Mandatory non-functional constraint to deliver a scalable and adaptable solution to dynamic threat environments.									
Source	Architectural Design Document (Development View)			Source Document	-					
Acceptance/Fit Criteria	The development structure (e.g., Component Diagram) must demonstrate that any core detection module (e.g., FR-DA-02) can be replaced or updated with minimal impact (e.g., $\leq 5\%$ code change) on the overall framework.									
Dependencies	Requires the Software Interfaces to be defined abstractly (e.g., via IDL).									
Priority	Essential	Conditional	-	Optional	-					
Change History	Initial Draft									

Table 18: Table for Functional Requirement 17

6 Nonfunctional Requirements & Software System Attributes

This section specifies the qualitative criteria and constraints that define the system's operational effectiveness, reliability, and security posture within a high-stakes, real-time environment.

6.1. Performance Requirements

These requirements define the necessary quantitative characteristics related to speed and capacity to ensure the **TrueSight** system operates effectively within the latency bounds of live communication services.

- **Real-Time Latency Constraint:** The verification process must adhere to stringent time constraints to mitigate deepfake attacks in real-time communications. The system must complete multi-modal analysis and render an authentication decision within an operationally defined minimum latency threshold.
- **Throughput and Scalability:** The system is explicitly required to deliver a scalable and resilient authentication solution. The performance architecture must accommodate high volumes of synchronous stream data associated with live communication services (e.g., video calls, VoIP).
- **Detection Accuracy:** The system's primary performance objective is the accurate detection and prevention of deepfake-based identity spoofing. A specific, quantifiable metric (e.g., Attack Presentation Classification Error Rate) must be met for detection precision.

6.2. Non Functional requirements

This subsection covers system attributes related to security, operational integrity, and forensic accountability, which apply across the system's architecture.

6.2.1. Security and Cybersecurity

- **Zero-Trust Mandate:** The system shall implement a mandatory zero-trust security architecture to secure all communication pipelines and enforce strict verification policies.
- **Advanced Defense Mechanisms:** Robust cybersecurity must be integrated, including AI-powered anomaly detection and Multi-Factor Authentication (MFA).
- **Behavioral MFA:** The MFA protocols must specifically incorporate behavioral biometrics, such as keystroke dynamics and voice stress analysis, to validate continuous identity.
- **Data Protection:** The system must enforce secure metadata management and protect sensitive biometric data.

6.2.2. Traceability and Accountability

- **Tamper-Proof Logging:** Digital forensic traceability must be ensured via blockchain-based evidence logging and tamper-proof logging mechanisms.
- **Forensic Watermarking:** The system must utilize forensic watermarking for generated logs and evidence to guarantee data integrity and accountability during post-incident analysis.
- **Source Attribution:** The solution must specifically support digital forensic investigations and the tracing of deepfake content origin.

6.2.3. Compliance and Modularity

- **Standards Compliance:** The proposed system is aligned with and must adhere to international biometric standards (e.g., ISO/IEC).
- **Architectural Modularity:** The system is inherently required to be modular, scalable, and resilient , designed for adaptation to evolving deepfake generation techniques.

7 Project Design/Architecture

- 4+1 ARCHITECTURE VIEW MODEL
 - Use Case View

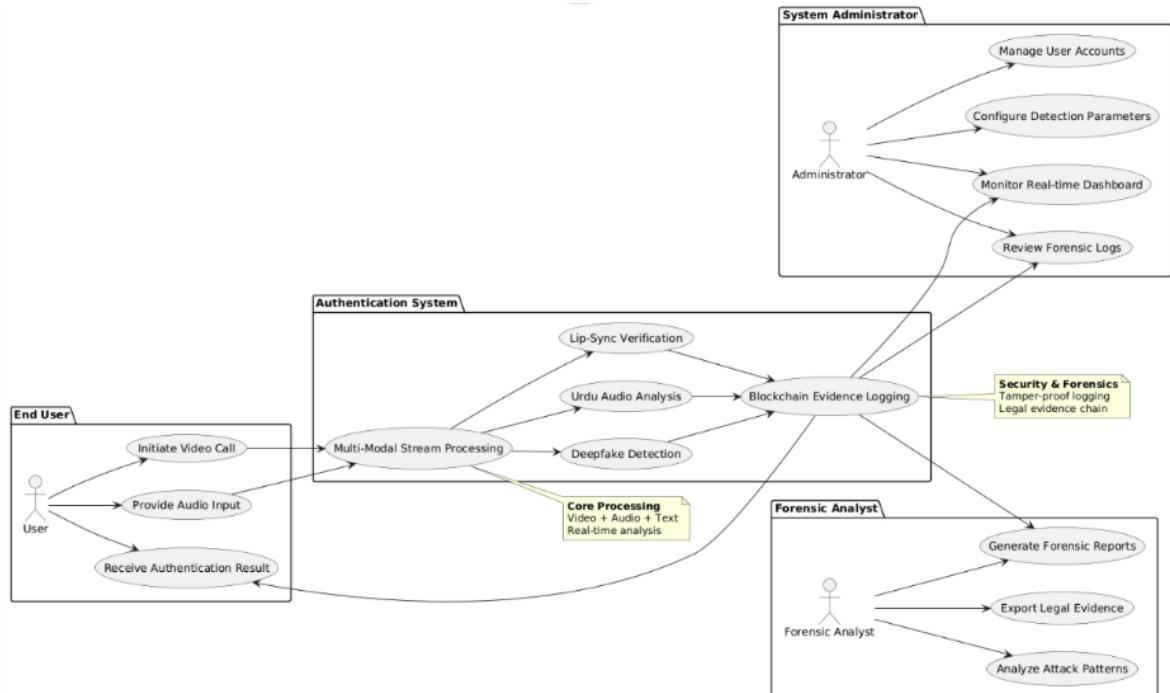


Figure 1 : Use Case View

TrueSight : AI – Powered Spoofing Detection and Source Identification System

○ Logical View

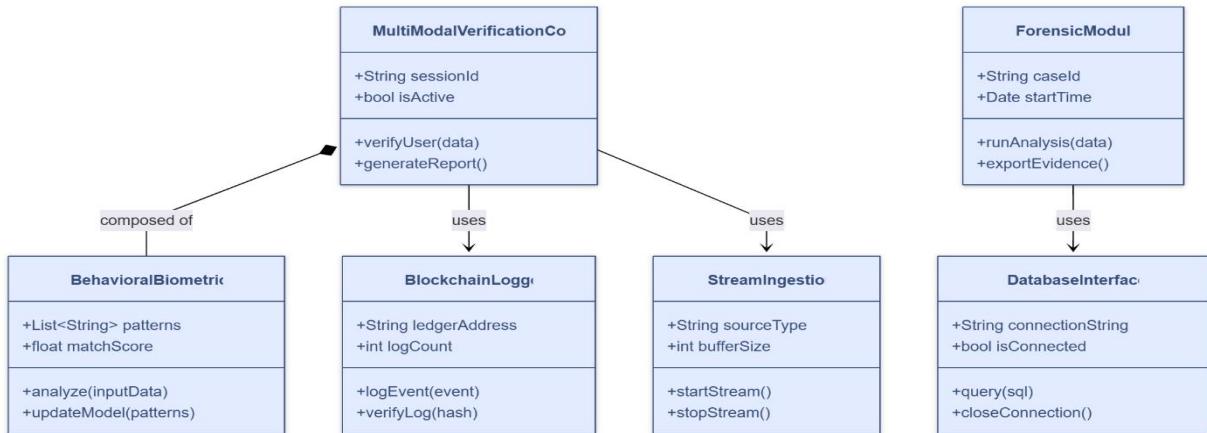


Figure 2 : Logical View

○ Development View

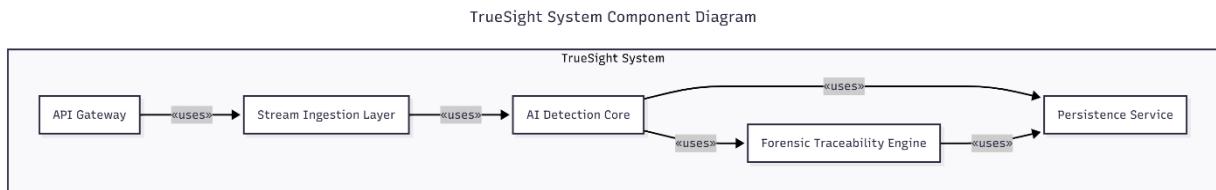


Figure 3 : Development View

○ Process View

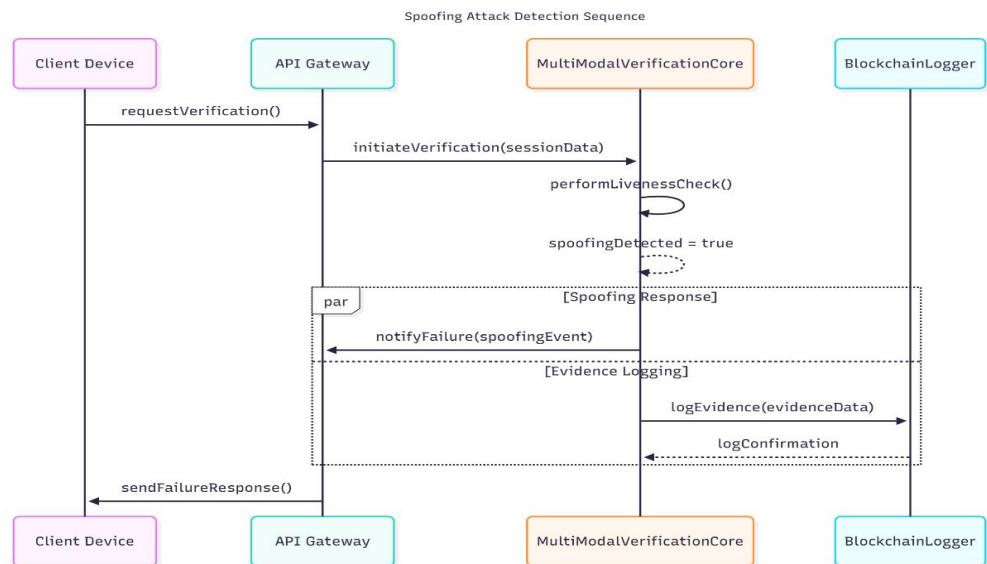


Figure 4 : Process View

TrueSight : AI – Powered Spoofing Detection and Source Identification System

- Physical View

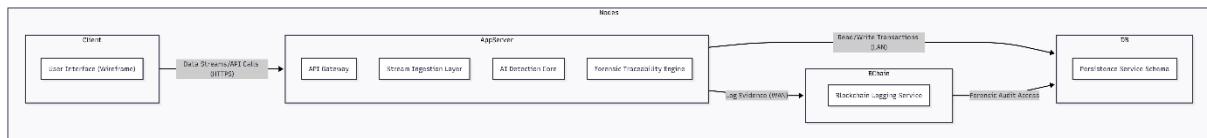


Figure 5 : Physical View

- State Machine Diagram

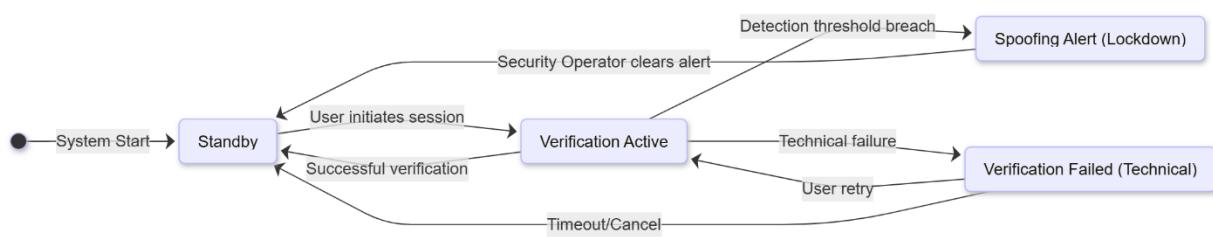


Figure 6 : State Machine Design

- ER Diagram

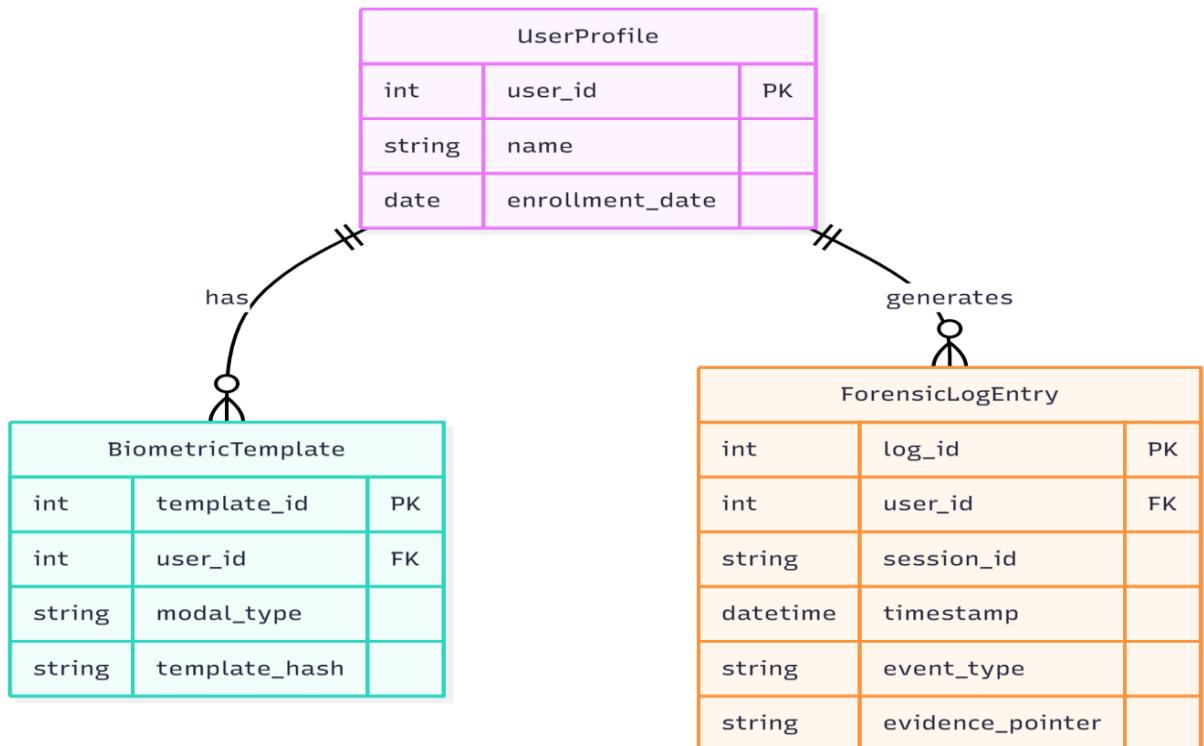


Figure 7 : ER Diagram

o Activity Diagram

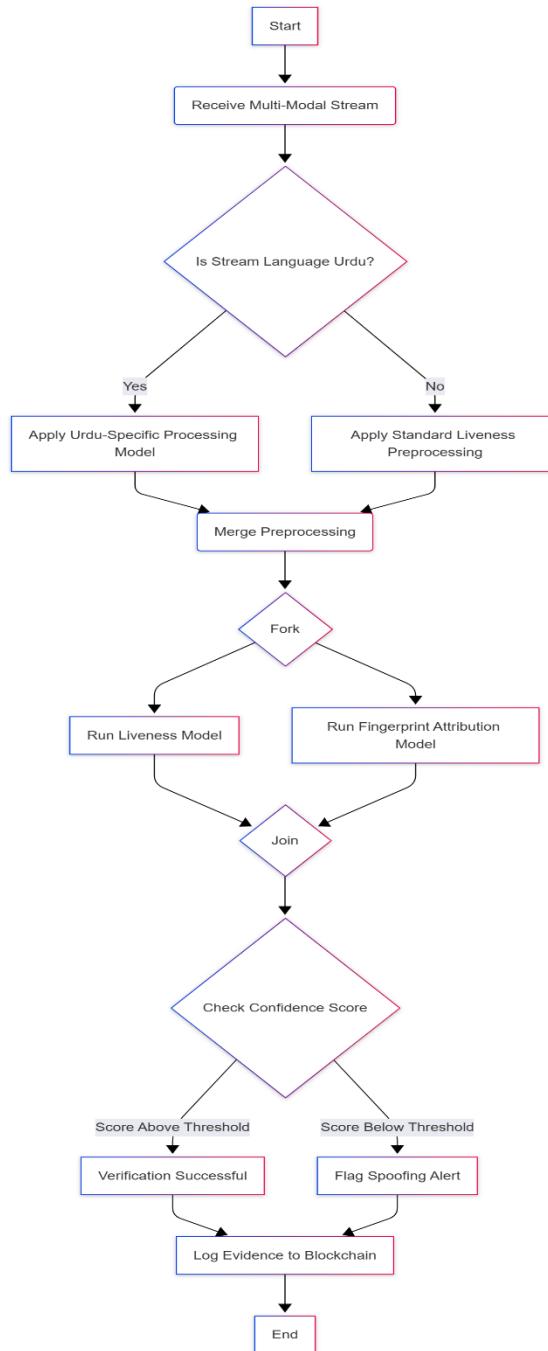


Figure 8 : Activity Diagram

User Interface Design :

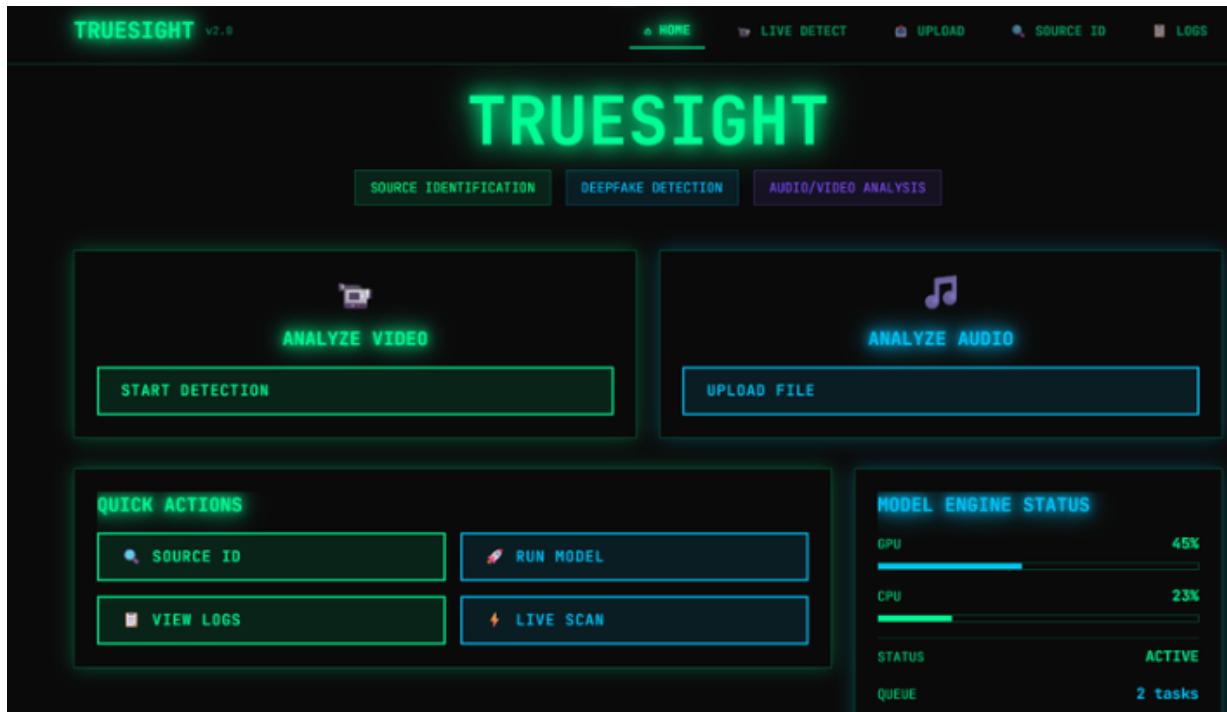


Figure 9 : User Interface Design