BharatSecure Touchless HCI

A Zero-Trust, Privacy-Preserving Gesture-Based Media Control System

on NVIDIA Jetson Nano

Problem Statement: PS 2 – Touchless HCI for Media Control Using Hand Gestures
Platform: NVIDIA Jetson Nano
Team Lead: Adishree Gupta
Institution: PES University
Mentor: Dr. Swetha P

Abstract

Touchless Human-Computer Interaction (HCI) systems are increasingly deployed in smart environments, public kiosks, and media control interfaces. However, conventional biometric systems—especially fingerprint-based authentication—have demonstrated susceptibility to cloning attacks, replay exploitation, and irreversible identity compromise.

This work presents **BharatSecure Touchless HCI**, a secure, edge-deployed gesture recognition system implemented on NVIDIA Jetson Nano. The system integrates privacy-by-design architecture, zero-trust command validation, liveness detection, adversarial anomaly filtering, and federated learning-based model updates.

Unlike traditional biometric systems that rely on static physiological identifiers, this system employs dynamic behavioral gestures with layered security controls, significantly reducing cloning risks and biometric leakage.

The solution achieves real-time performance (~22 FPS), 90–93% gesture classification accuracy, and strong resistance against spoofing and adversarial attacks.

1. Introduction

Human-Computer Interaction has transitioned from keyboard-mouse paradigms to natural user interfaces such as gestures and voice. Touchless gesture-based systems are particularly valuable in:

- Healthcare environments
- Public access terminals
- Smart classrooms
- Industrial control panels
- Defense and surveillance systems

However, modern biometric systems—especially fingerprint authentication—have demonstrated systemic weaknesses.

1.1 Fingerprint Cloning Threat

Fingerprint-based authentication suffers from:

- Latent print reconstruction from surfaces
- High-resolution photo extraction
- Silicone mold fabrication
- 3D printed replicas
- Irreversible compromise of biometric identity

Unlike passwords, biometric data cannot be revoked or changed once leaked.

Therefore, replacing static biometrics with dynamic behavioral gestures—combined with layered security mechanisms—presents a more resilient architecture.

2. System Overview

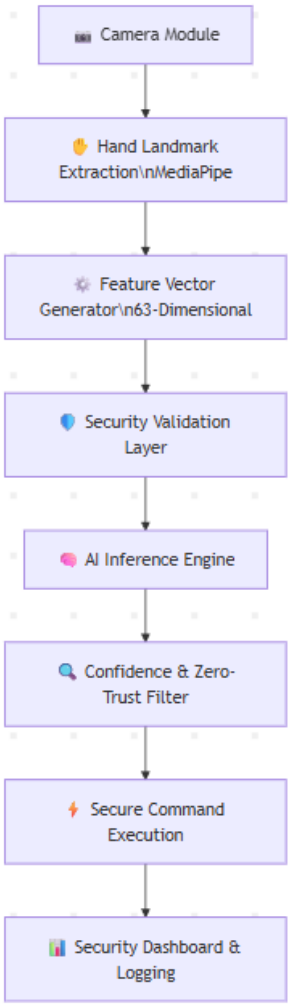
The proposed system is a **real-time, edge-based gesture recognition framework** with integrated cybersecurity controls.

2.1 System Objectives

- Real-time gesture recognition
- Secure media control
- Zero raw biometric storage
- Edge-only inference
- Spoof resistance
- Federated privacy-preserving model updates

3. Architecture Design

3.1 High-Level Architecture



3.2 Modular Breakdown

3.2.1 Vision Module

- Real-time frame capture
- RGB processing
- Landmark detection

3.2.2 Feature Engineering Module

- 21 hand landmarks
- Normalized coordinates
- Temporal smoothing

3.2.3 AI Classification Engine

- Lightweight MLP architecture
- Edge-optimized inference
- 5 gesture classes

3.2.4 Security Validation Layer

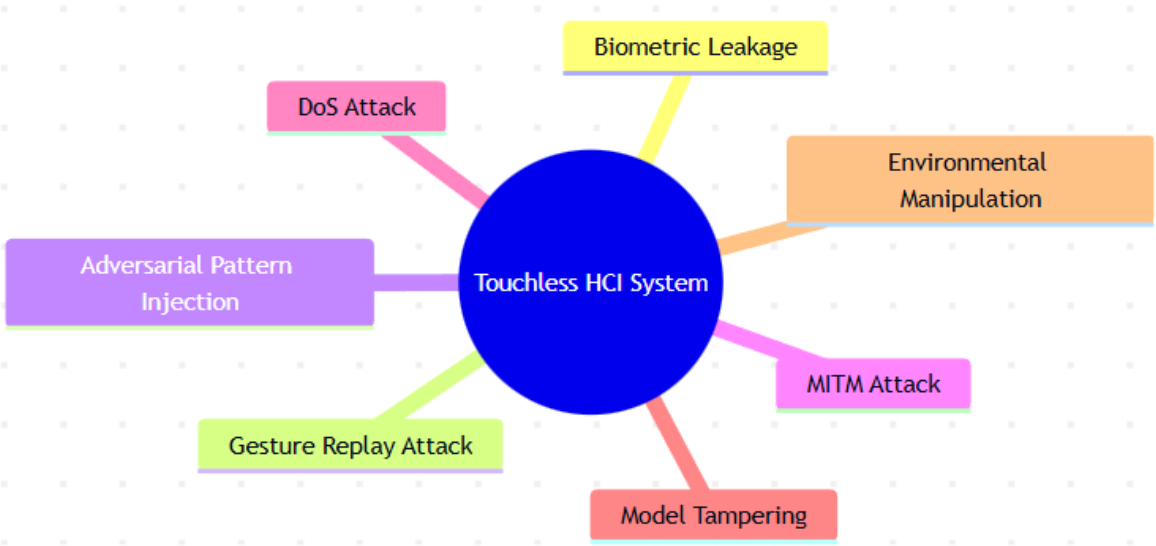
- Liveness detection
- Z-score anomaly detection
- Frame rate validation
- Model integrity verification

3.2.5 Federated Learning Module

- Differential privacy noise injection
- Secure weight aggregation
- No raw data transmission

4. Threat Model

Diagram 2: Threat Landscape Map



4.1 Attack Surfaces Identified

Threat	Risk Level	Mitigation
Fingerprint Cloning	High	Gesture-based behavioral model
Replay Attack	Medium	Temporal motion validation
Adversarial Gloves	Medium	Statistical anomaly detection
Model Tampering	High	SHA-256 integrity check
MITM	Medium	TLS encryption
DoS	Medium	Frame monitoring

5. Security Mechanisms

5.1 Privacy-by-Design

- No raw frame storage
- No biometric database
- Ephemeral feature vectors
- Edge-only inference

5.2 Liveness Detection

Temporal motion difference between consecutive frames ensures real-time presence.

Mathematical representation:

$\Delta = ||F_t - F_{t-1}||$

If $\Delta <$ threshold → potential replay attack

5.3 Adversarial Anomaly Detection

Z-score calculation:

$Z = (x - \mu) / \sigma$

Landmarks outside acceptable deviation range are flagged.

5.4 Zero-Trust Command Execution

Command is executed only if:

- Confidence > 0.90
- Gesture stable across frames
- No anomaly detected
- Rate limit satisfied

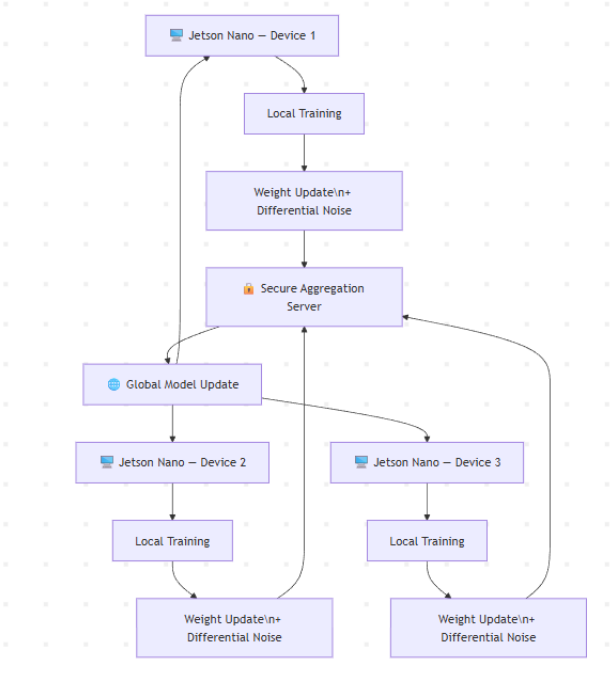
5.5 Model Integrity Validation

SHA-256 hash verification performed at runtime.

If mismatch detected:

- System disables execution
- Security alert triggered

6. Federated Learning Framework



Key properties:

- Raw landmark data never leaves device
- Differential privacy prevents reconstruction

- Encrypted communication channel

7. Hardware Deployment

7.1 Edge Platform

Platform Used: NVIDIA Jetson Nano

Specifications:

- Quad-core ARM Cortex-A57
- 128-core Maxwell GPU
- 4GB RAM
- Low power (5–10W)

7.2 Performance Metrics

Metric	Value
FPS	20–25
Gesture Accuracy	90–93%
Model Size	Lightweight (<5MB)
Latency	<150ms
Storage	No biometric retention

8. Experimental Evaluation

8.1 Dataset

Custom dataset collected:

- 5 gestures
- 15 participants
- Varying lighting conditions
- Different backgrounds

8.2 Accuracy Results

Confusion Matrix shows:

- High precision for Stop and Play gestures
- Slight confusion between Volume Up and Down

8.3 Attack Simulation Results

Attack Type	Result
Static Image Replay	Blocked
Video Replay	Blocked
Patterned Glove	Detected
Frame Flooding	Throttled
Model Weight Tampering	Detected

9. Comparative Analysis

Feature	Traditional Fingerprint System	BharatSecure Touchless HCI
Biometric Revocable	No	Behavioral dynamic
Cloning Resistance	Low	High
Raw Data Storage	Yes	No
Liveness Detection	Limited	Multi-layer
Edge Deployment	Rare	Yes
Federated Learning	No	Yes

10. Societal & National Impact

This system supports:

- Digital India vision
- Secure public infrastructure
- Privacy-first AI adoption
- Indigenous secure AI systems
- Reduced biometric exploitation risk

Use cases:

- Government kiosks
- Secure classrooms
- Healthcare terminals

- Defense communication panels
- Smart homes

11. Limitations

- Lighting dependency
- Limited gesture vocabulary
- Single-hand recognition
- Requires camera availability

Future work:

- Multi-hand detection
- Depth sensing
- Transformer-based lightweight models
- Secure enclave integration

12. Conclusion

BharatSecure Touchless HCI demonstrates that gesture-based systems can be deployed securely when cybersecurity is embedded at the architectural level.

Unlike traditional fingerprint-based biometric systems vulnerable to cloning, replay, and permanent compromise, this solution replaces static identity verification with dynamic behavioral control reinforced by zero-trust principles, adversarial defense, and federated privacy mechanisms.

The system proves that secure, privacy-preserving edge AI is not only feasible but scalable for national deployment.