DeepShield: Biometric-Based Anti-Deepfake Login System for Secure Banking

In today's interconnected world, online banking has become an indispensable part of our lives. However, this convenience comes with increasing security challenges. The rise of sophisticated cyber threats, particularly deepfake technology, demands innovative solutions to protect sensitive financial data.

This presentation introduces DeepShield, a cutting-edge biometric-based anti-deepfake login system designed to safeguard online banking platforms against evolving threats. We will explore the vulnerabilities of current systems and how DeepShield leverages advanced AI and liveness detection to ensure robust authentication.

Abstract: Unveiling DeepShield

System Overview

DeepShield is an innovative system engineered to fortify online banking security by preventing deepfake-based biometric attacks.

Core Purpose

Its primary objective is to authenticate legitimate users while effectively detecting and rejecting sophisticated deepfake attempts across various biometric modalities.

Key Technologies

The system integrates state-of-the-art biometrics, artificial intelligence (AI), machine learning (ML) algorithms, and advanced liveness detection techniques.

The Deepfake Threat in Banking

Rise of Deepfake Fraud

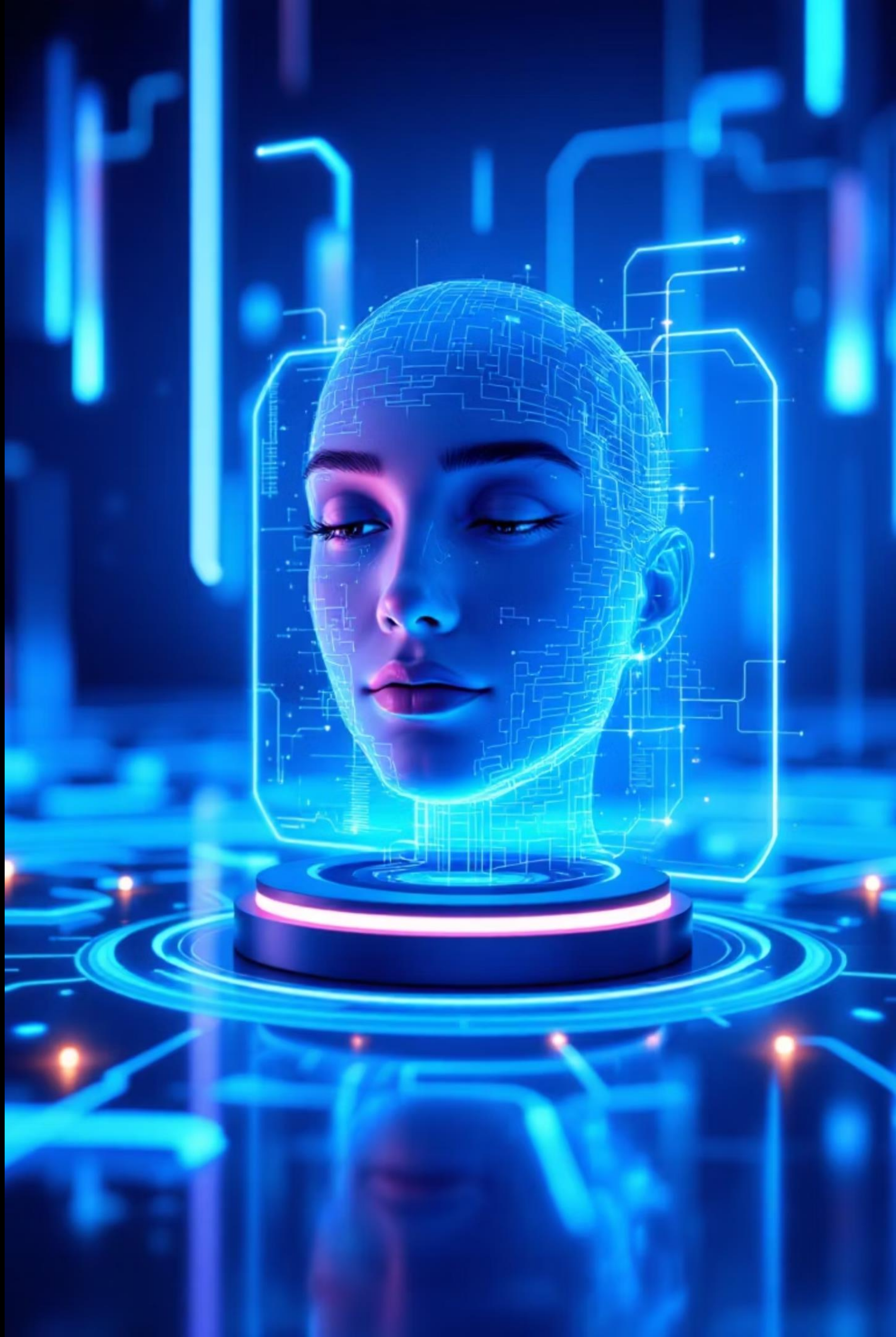
Sophisticated AI-generated attacks are targeting traditional biometric systems.

Face & Voice Spoofing

Deepfakes can mimic users' faces and voices, bypassing standard authentication.

Traditional Biometrics Fail

Current systems lack the advanced liveness detection needed to counter deepfakes.



LITERATURE REVIEW

Foundations: Existing Biometric Authentication Systems

Facial Recognition

Utilizes unique facial features for identification. Common in smartphones and some banking apps.

Fingerprint Scanning

Analyzes unique ridge patterns. Widely used due to its convenience and perceived security.

Voice Recognition

Authenticates based on unique vocal characteristics. Gaining traction for remote authentication.

Iris/Retinal Scans

Highly accurate methods based on unique eye patterns, often used in high-security environments.

While these systems offer convenience and improved security over passwords, they are not immune to sophisticated spoofing techniques. The static nature of the recorded biometric data makes them vulnerable if the data falls into the wrong hands or if deepfakes are used.

LITERATURE REVIEW

The Adversarial Landscape: Deepfake Generation & Detection

Deepfakes are synthetic media in which a person in an existing image or video is replaced with someone else's likeness using artificial intelligence. This technology, primarily built upon generative adversarial networks (GANs), has made significant strides in creating hyper-realistic forgeries.

Deepfake Generation Techniques

- Generative Adversarial Networks (GANs): Pit two neural networks against each other to create realistic fakes.
- Autoencoders: Encode and decode data, often used for face-swapping.
- Voice Cloning: Synthesizes a person's voice from a small audio sample.

Current Detection Approaches

- Forensic Analysis: Examining artifacts, inconsistencies, or subtle distortions in media.
- AI-based Classifiers: Training models to recognize patterns specific to synthetic media.
- Physiological Signal Analysis: Detecting lack of natural physiological responses (e.g., blinking, pulse).

LITERATURE REVIEW

Bridging the Gap: Limitations of Current Anti-Spoofing

While deepfake detection is an active research area, current anti-spoofing and liveness detection methods face several limitations that DeepShield aims to address.

Static Feature Reliance

Many existing systems primarily analyze static features, which can be overcome by advanced deepfake generation that accurately replicates these features.

Vulnerability to New Deepfake Models

Detection models trained on older deepfake datasets may not perform well against newer, more sophisticated deepfake generation techniques.

Lack of Multi-Modal Integration

Most solutions focus on a single biometric modality, leaving other modalities vulnerable to attack.

Performance in Real-World Scenarios

Challenges in deploying robust liveness detection in diverse environments with varying lighting, angles, and user behavior.

DeepShield addresses these limitations by incorporating a multi-layered approach, combining advanced AI with real-time liveness analysis across multiple biometric inputs.

DeepShield: Our AI-Powered Solution

DeepShield is an AI-powered, multi-modal biometric system designed to protect banking logins from deepfake attacks.

Multi-Modal Verification

Combines face, voice, and behavioral biometrics for robust security.

AI-Powered Liveness

Advanced AI detects subtle signs of liveness to thwart spoofing attempts.

Future-Ready Defense

Continuously adapts to new deepfake techniques, ensuring long-term protection.

How DeepShield Works: A Secure Authentication Flow

DeepShield employs a sophisticated multi-stage process to ensure the authenticity of a user's biometric login attempt.

Biometric Data Capture

The system captures live biometric data (e.g., face scan, fingerprint, voice sample) from the user at the point of login.

Preprocessing & Feature Extraction

Raw biometric data undergoes noise reduction, normalization, and extraction of unique features relevant for identification and liveness analysis.

AI-Based Deepfake Detection & Liveness Analysis

Advanced AI/ML models analyze extracted features in real-time to detect subtle cues indicating a deepfake and verify the liveness of the biometric input.

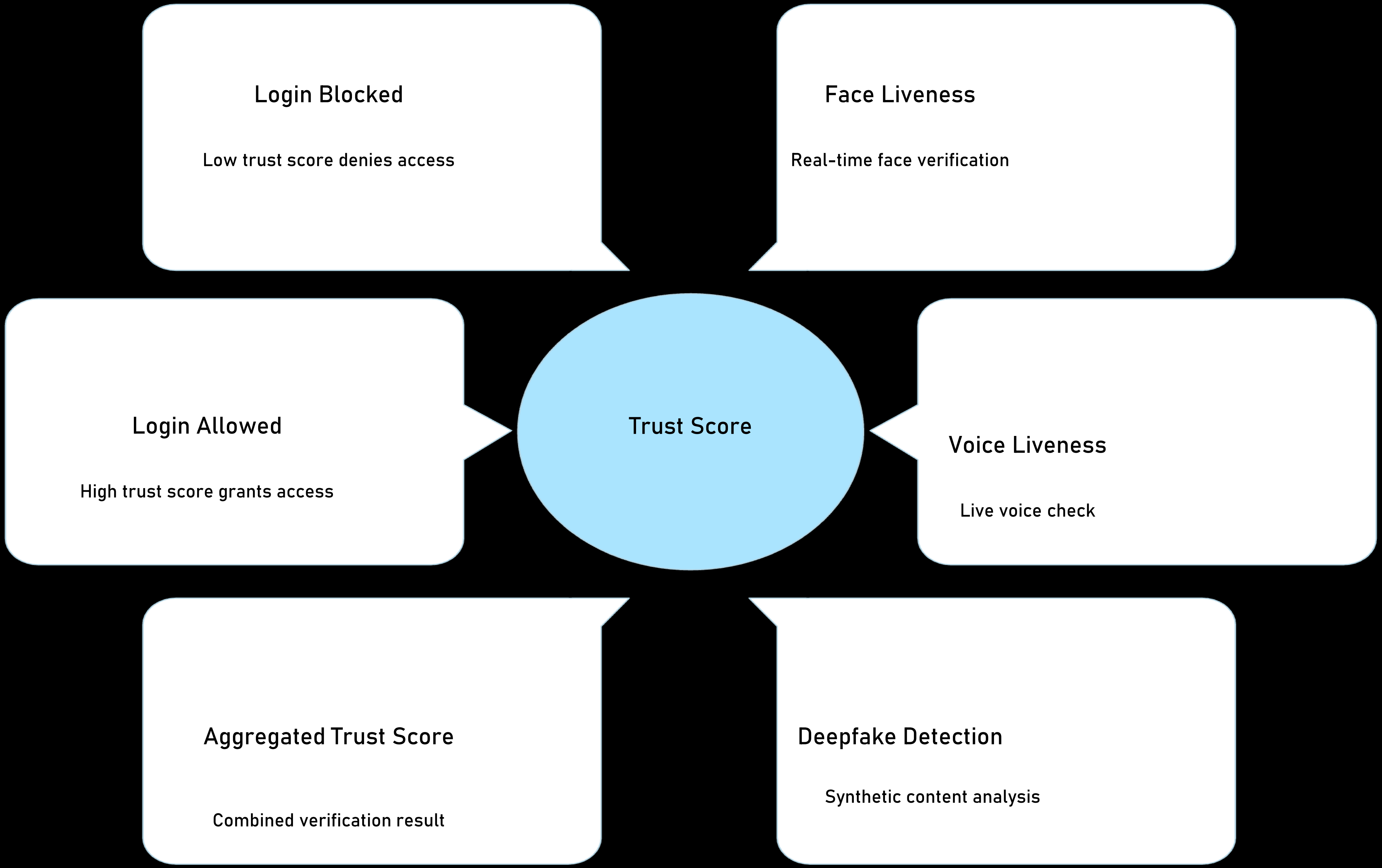
Authentication Decision

Based on the analysis, the system determines if the biometric input is genuine or a spoof attempt.

Secure Login Approval/Rejection

If genuine, login is approved; otherwise, it is rejected, and an alert may be triggered.

The Trust Score: Informed Login Decisions



Trust Score

Login Blocked

Low trust score denies access

Face Liveness

Real-time face verification

Login Allowed

High trust score grants access

Voice Liveness

Live voice check

Aggregated Trust Score

Combined verification result

Deepfake Detection

Synthetic content analysis

Adaptive and User-Friendly Security

Designed for Genuine Users

The system prioritizes user experience, ensuring that temporary voice issues or minor illnesses do not unfairly block legitimate access.

Dynamic Adaptability

It dynamically adjusts to varying conditions, maintaining a high level of security without compromising accessibility.

Key Advantages of DeepShield

Strong Protection

Robust defense against sophisticated deepfake and presentation attacks, significantly reducing the risk of unauthorized access.

Enhanced Banking Security

Elevates the overall security posture of online banking platforms, protecting sensitive financial data and customer trust.

Reduced Fraud & False Acceptance

Minimizes instances of fraudulent logins and significantly lowers the false acceptance rate (FAR) for biometric authentication.

Scalable & Future-Ready

Designed with a modular and adaptable architecture, allowing for easy integration of new biometric modalities and continuous updates to counter evolving deepfake technologies.

Thank You !

We hope this presentation has provided a comprehensive overview of the DeepShield system and its critical role in securing the future of online banking.