Gatekeeper Engine

Power your application with the world's fastest, most accurate voice biometrics.

Gatekeeper Engine is built on 4th-generation deep neural networks and can authenticate a person's identity with as little as 1 second of audio, perform real-time ID&V, and support large-scale complex data mining operations.

Powering security with voice biometrics

Gatekeeper Engine puts Nuance's industry-leading voice biometrics technology in your hands through an easy-to-integrate standardized API. Enterprises building applications in public security, identification and verification (ID&V), and fraud prevention use Gatekeeper Engine to add the world's fastest, most accurate voice biometrics capabilities to their solutions.

Enterprises turn to Gatekeeper Engine when they know that only the best voice biometrics technology will suffice. And by choosing Nuance, you are aligning yourself with a proven partner building the future of voice biometrics, intelligent authentication, and fraud prevention. We are constantly investing in our core technology and we pass those improvements to you, while giving you direct access to our team of world-class tech experts who will support you however and whenever with resources, best practices, and more.

Features

— **Voice biometrics**
Our latest voice biometrics engine, Nuance Lightning Engine, uses 4th-generation deep neural networks to deliver the world's fastest and most accurate voice biometrics performance. In your hands, our voice biometrics can authenticate a person's identity with as little as 1 second of audio and is easily capable of real-time ID&V and large-scale data mining applications.

— **Synthetic speech detection**
Gatekeeper Engine analyzes input speech samples and calculates the likelihood that they were tampered with through voice morphing, adaptive text-to-speech (TTS), or high-quality TTS sampling. If the returned score exceeds a configured threshold, the system generates an alert to your application.

— **Playback detection**
Gatekeeper Engine tests incoming audio to see if it represents live speech or if it uses a recording that impersonates an authorized speaker. Channel playback detection detects the presence of signal artifacts introduced by

USE CASES

Integrate Gatekeeper Engine into your application for:

— **Identification and verification**
Validate that people really are who they claim to be, based on the unique characteristics of their voice. Authenticate someone in as little as 1 second from a vocal password, or authenticate them in the background as they're using the app.

— **Fraud prevention**
Raise the barrier against fraudsters with security factors that are impossible to circumvent or cheat, detect cases of fraud in real-time, and perform post-facto analyses to identity persistent fraudsters.

— **Public security**
Use segmentation, voice biometrics and cluster analysis to identify persons of interest in large databases of video and audio recordings and to gather evidence for use in law enforcement investigations.

the recording and playback process, and isolates playback attacks based on a user-defined false alarm rate. Footprint playback detection determines if two audio buffers correspond to the same utterance. The system compares the current audio with a saved "footprint" of a previously collected verification passphrase. If the two footprints match too closely, the current one is marked as a recording.

— **Language identification**
Gatekeeper Engine determines the language spoken within an audio sample even in natural speech contexts, enabling you to segment and cluster speakers based on their language even without any directed speech input.

— **Voice classification**
Gatekeeper Engine enables you to build custom categories and groups to bucket voices into based on other characteristics that are relevant to your application or field, such as age, gender, or even regional dialect.

— **Segmentation and clustering**
Gatekeeper Engine includes tools for segmenting speakers within a crowded audio file, and then using voice biometrics and clustering to identify individuals and analyze their voiceprints across datasets.

— **Platform support and deployment**
Gatekeeper Engine supports Windows, Linux, Android and iOS platforms, and can be deployed on-premises, in private or public clouds, or embedded for on-device processing.

— **Turnstile API**
Gatekeeper Engine is written using the Nuance Turnstile API. Turnstile functions as a unified interface to all Nuance engines and consists of a generic library that executes high level tasks above the core voice biometrics capabilities. Once your team becomes familiar with Turnstile for Gatekeeper Engine, you can easily incorporate other Nuance engines in the future. Through Turnstile, the Gatekeeper Engine API is available in C++ and Java.

LEARN MORE

Visit www.nuance.com/security-suite or email cxexperts@nuance.com.

UNDISPUTED MARKET LEADER

Today, more than 500 enterprises have –

Collected over

600M

voiceprints

Processed over

8B

consumer engagements

Achieved more than

$2B

in fraud savings every year.

Third parties consistently find that Nuance customers report better ROIs, higher fraud loss savings, and higher authentication success rates than organizations deploying competing solutions. Nuance is the only biometric security provider whose solutions have led to fraudsters being prosecuted and convicted for their crimes.

About Nuance Communications, Inc.
Nuance Communications, Inc. (NASDAQ: NUAN) is a technology pioneer with market leadership in conversational AI and ambient intelligence. A full-service partner trusted by 90 percent of U.S. hospitals and 85 percent of the Fortune 100 across the globe, we create intuitive solutions that amplify people's ability to help others.

ENT_4195_01_DS, Oct 1, 2020