Aculab Biometric Technologies

Datasheet

The Next Generation of AI Driven Biometric Authentication

Aculab's Biometric Technologies are designed to enable the efficient authentication of individuals via their face and/or voice. Your business's customers can replace frustrating, time-consuming processes simply by allowing their customers and/or employees to authenticate with their voice and/or face.

Across all market sectors, businesses compete in terms of customer experience. All seek efficiency and productivity gains. The simplicity and convenience of authenticating via voice and/or face, as opposed to agent-led Identity & Verification (ID&V) or Knowledge, and Token-Based Authentication (KBA or TBA), provides seamless user interaction, while also offering time and cost savings for the end user organisation.

With the escalation in identity theft, fraud, and social engineering attacks, businesses have a compelling imperative to provide enhanced security in terms of access to user data, accounts and services, for both employees and customers.

Aculab biometric technologies offer a solution; enabling voice, face, or the combination of both, to authenticate users and prevent fraudulent activity.

Aculab Biometric Technologies

The AI-Driven technology consists of three authentication systems

VoiSentry	FaiSentry	SentryFusion
Highly secure AI driven voice biometric system. Uses voice signatures to streamline the identification and verification process. Frees up time for agents, boosting operational productivity and driving tangible business results. Additionally, it helps to mitigate fraud risk; protecting customers and saving businesses money.	Highly secure AI driven face recognition system. Eliminates the need for passwords and facilitates frictionless authentication for unparalleled user experience. The technology can identify multiple individuals from a single image, with results in under a second. The solution is impervious to race and gender biases.	Highly secure AI driven multimodal biometric system. Enables Video & Audio data to be analysed in unison, verifying individuals on a higher security level. Includes a cluster-based architecture, providing effective scalability, robustness and future-proofing, along with the option of hosting on-premise or in a data centre.

Key features

Easy Integration	A 'virtual appliance' for deployment as a VM on the developer's platform of choice; on-premise, data centre, or hosted cloud
Voice and/or image identification	The option to identify rather than verify someone from their voice and/or face
REST APIs	Applications can be written in the developer's programming language of choice
Anti-spoofing	Mitigates risks from mimicking and faked data attacks
Text independent	Verification can be continued throughout a call
User verification	Verify callers against an identity claim
User identification	Identify a speaker from a list of known candidates

Multiple verification modes	Text-dependent, text-independent, and text-prompted modes, all using the same speaker models
Autonomous passphrases	Individual passphrases provide an additional level of security
Multi-factor authentication	Integrated, multi-lingual spoken number and DTMF recognition
Presentation attack detection	Anti-spoofing technology mitigates risks from presentation attacks, including synthesised and replayed speech
Algorithmic adaptation	Per-speaker adaptation and model updating track changes in the user's voice and improve accuracy
Machine learning and artificial intelligence (AI)	Combines machine learning and AI with hand-crafted algorithms and advanced signal processing for robustness and accuracy
Web-based UI	All nodes accessible from a log-in at a single node; remote, web-services administration
Multi-tenant	Runs multiple, distinct applications, and hosted solutions
Scalable and redundant	Add capacity and redundancy via a multi-node system
Load balancing	Optimise system node throughout, loading and response time

Product benefits

Self-service assist (IVR containment) - simple, convenient, intuitive verification by voice and/or image

Improves the customer experience (CX) - reduces the irritating security interrogations

Cost-effective and efficient - dramatically reduced time/cost compared to manual KBA

Multi-factor authentication - enables & enhances security and fraud prevention

Flexible deployment - ideal for multiple, distinct applications, and hosted solutions

For developers of solutions requiring secure identity verification, or providers offering services to multiple clients from their hosted, cloud- based platforms, Aculab Biometric Technologies presents an ideal solution.

A multi-tenant customer interaction solution, for example, can offer caller ID&V, simply and conveniently, according to individual businesses' needs. Each business has full, independent control over the creation of datasets against which enrolments and verification or identification attempts are performed.

Technical Summary

Minimum Hardware Configuration	
Processor	8 CPU cores
Memory	20GB RAM (including 4GB system headroom) / 16 GB RAM (24GB if video is used)
Storage	20GB of VM disk storage (when using the integrated volume)

Software Environment	
Deployment	Virtual appliance for deployment as a VM (ideally sole VM) onto a hardware platform with an installed virtualisation hypervisor; alternatively, as a 'Docker image'
Hypervisor	VMWare vSphere ESXi 6.0, or ESXi 6.5; Microsoft Hyper-V; Docker (Linus host)
Application Programming Interface (API)	Web-services, REST-based API
User Interface (UI)	HTML-based administration UI (allows administrative control and status visibility over an entire cluster)
Web-services (WS)	A WS-based administration REST interface (enables remote administration from 3rd party applications)
Data Storage	Self-contained volume (within the virtual appliance); alternatively, greater external capacity may be assigned
Additional Specifications	
Encryption	All voice and image data can be encrypted
Voice models	Not externally accessible; proprietary format
Face models	Not externally accessible; proprietary format
Voice Passphrase	Fixed, or autonomous selection (applies to text-dependent)
Voice verification modes	Text-dependent and text-independent; API based
Identification	Identifies a speaker from a list of known candidates
Liveness detection	Through prompts and/or multi-factor authentication
Similarity (anti-spoofing)	Performs a similarity (duplicate/copy) test on audio data

Presentation attack detection (PAD)	Selectable; duplicate, replayed or synthesised speech (ref: ISO 30107-3)
Languages	Language independent
Minimum input	2 seconds of speech
Recommended enrolment	3 repetitions
Recommended verification	1 repetition
Enrolment time	Sub-second (for 3 repetitions of a passphrase of 3 seconds)
Verification image	1 image of the face
Enrolment images	3 different images of the face
Voice verification time	0.5 seconds
Image verification time	Less than 2 seconds
Voice & image (video) verification time	3 seconds
Verification latency	Sub-second (for a passphrase of 3 seconds)
Identification latency	Dependent on comparison ratio
Audio format	.wav format; G.711 (A-law or μ-law) or 8kHz, 16-bit linear 9mono) PCM
Image format	JPEG (JFIF or Exif) preferred. GIF is not supported
Video format	Mp4 preferred
Feature analysis	Designed for real-world telephone speech, sampled at 8kHz; noise robust
Voice only verification throughout	A standard configuration; has been proven at up to 40,000 verifications per hour
Image only verification throughout	11,000 verifications per hour on a standard configuration
Video verification throughout	7,000 verifications per hour on a standard configuration
Identification performance	In excess of 40,000 comparisons per hour; ratio dependent
Verification accuracy	A system has been shown to have an imposter detection rate of 99.65%
Equal error rate (EER)	A system has been shown to have an EER of <2%
Anti-spoofing	Audio and video spoof detection

Model adaptation	Models can be updated and enhanced with new data
Algorithmic adaptation	Dynamic, per-speaker adaptation and model updating
Sensitivity threshold	API configurable
Voice identification	Identifying one out of 100 models, 3,300 per hour
Face identification	Identifying one out of 100 models, 4,500 per hour
Voice & face identification	Identifying one out of 100 models, 2,000 per hour
Automatic speech recognition	Selectable (digits 0-9; 'yes' and 'no' - English; French; German; Spanish; Italian)
DTMF detection	Selectable
Security threshold	Configurable
Scalability	Capacity scales linearly with number of cluster nodes
Resilience & redundancy	Failover protection via clustering nodes
Load balancing	Reverse proxy; node polling
Management	Monitored/managed from administrator log-in at single node
Licensing	Embedded licence server

Notes:
1. A cluster consisting of a single node running as a sole guest under VMWare ESXi 6.0 on an Intel i7 at 3.2GHz, and assigned all 4 cores (8 hyperthreaded cores) and 12GB RAM (also used by the hypervisor) with a local SSD.
2. SentryFusion has been evaluated using numerous voice, image and video databases, covering a wide range of recording equipment and environments.
3. The number of false acceptances being equal to the number of false rejections.

For more information, please contact your Account Manager or view our website: http://www.aculab.com

Specifications may change; this product overview is for informational purposes only. Aculab makes no warranties, express or implied, in this document. E&OE.