WHITE PAPER

Acoustic sensor for audio analytics

May 2025

AXIS COMMUNICATIONS

Summary

To alleviate privacy concerns about audio but still benefit from the many advantages of edge-based audio analytics, there are cameras with an acoustic sensor instead of a microphone. The acoustic sensor allows audio analytics in the camera to scan and measure sound waves but not stream or store audio. The output from the analytics is audio metadata such as decibel levels, frequency information, and other types of non-personal data that can be set to trigger alerts and events in the camera.

Cameras with an acoustic sensor have a software barrier implemented, eliminating access to audio services. For example, AXIS OS has no audio streaming APIs for the acoustic sensor. This means that neither users nor applications can initiate streaming or storing of audio.

When it comes to products and solutions sold by Axis, it's the user of the product or solution that is responsible for making sure that any use of the product is compliant with applicable privacy laws. Axis strives to design products to make it easier for you to be compliant. By providing cameras with an acoustic sensor and software barrier Axis enables a more privacy-friendly solution for audio monitoring, which allows audio data analysis without streaming or storing sensitive audio information.

Table of Contents

1 Introduction

If your camera has an acoustic sensor instead of a microphone, the camera doesn't stream or store any audio. The sensor allows audio analytics in the camera to detect and measure sound waves for analytics on the edge but no sensitive audio data can be stored or accessed by any user.

This white paper presents what an acoustic sensor is and outlines the possibilities it provides.

2 Background

2.1 Audio analytics

Audio analytics analyze sound characteristics to generate non-audio output.

Audio analytics are used to detect for example screams, glass breakage, and sudden changes in audio level. You can use audio analytics separately or in combination with video surveillance.

If you use video analytics, adding audio analytics means enabling another dimension of awareness that can significantly increase the detection confidence. This is the case especially if the video analytics is challenged by circumstances such as poor light conditions.

A system that combines audio analytics with video surveillance can, for example, alert operators to ongoing potential incidents and guide them to the relevant camera views. This can enable early detection, swift intervention, and in many cases, prevention of further escalation of incidents. Audio analytics can create automated events that not only save time and cost but also protect personal integrity.

2.1.1 Privacy with audio analytics

In many environments there are concerns regarding the use of microphones in video surveillance. These concerns are typically linked to the recording of plain speech along with the video material, or the possibility for someone to listen to private conversations. Laws regulating surveillance can also be different depending on whether audio data or video data is used.

But there's a difference between detecting sounds and recording them. Audio analytics don't record incoming audio, nor transmit it from the camera. Instead, they just search for specific patterns, levels, or frequencies. When analytics run on the edge (in the camera), no audio needs to leave the camera - only the results from the performed analytics, that is, metadata or triggers, do.

3 The acoustic sensor

With an acoustic sensor the camera has no support for streaming or recording audio. Analytics installed in the camera can scan the incoming audio to produce metadata, but no audio leaves the camera. Audio analytics is the only audio use case. The only output is audio metadata, such as decibel levels, energy in different frequencies over time, alerts, and events. Because a camera with an acoustic sensor doesn't stream or store any personal data, you minimize the risk of infringing on anyone's rights to privacy.

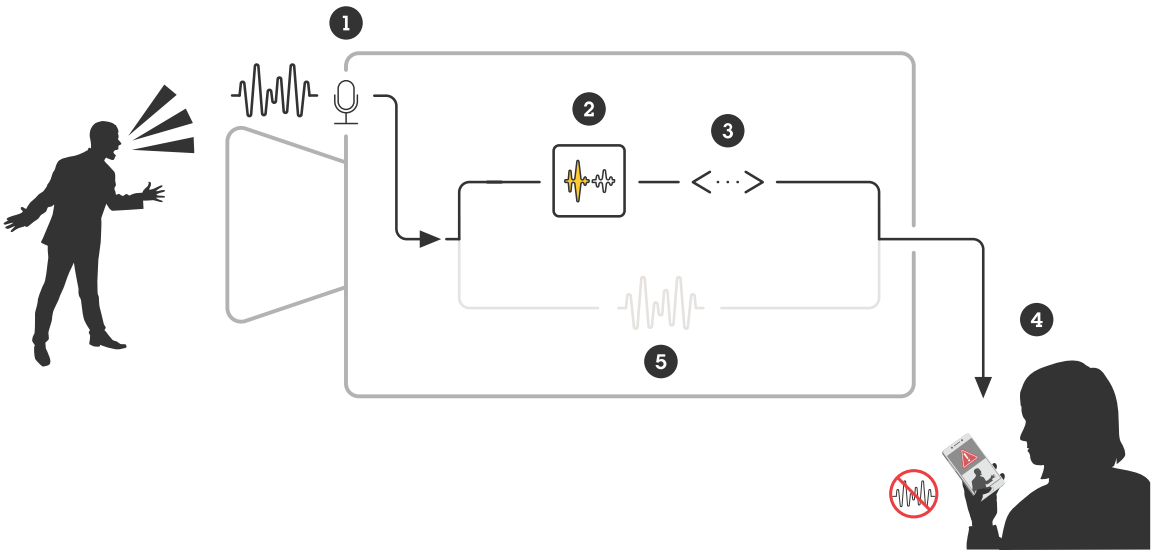

Figure 3.1 *A camera with acoustic sensor, from scanning sound waves (1) to alerting a user (4).*

1 *The acoustic sensor microphone scans sound waves.*
2 *The audio analytics detects decibel levels, screaming, or shouting (or what the specific analytics is searching for).*
3 *Metadata, including an event notification, is generated by the audio analytics.*
4 *Stakeholders can configure to receive an alert based on the event notification and metadata. They can verify by checking the video stream.*
5 *No audio stream is available.*

4 AXIS OS in cameras with acoustic sensor

Axis devices run the operating system AXIS OS. It's Linux based and it normally uses standard Linux audio (ALSA/PipeWire). Cameras with an acoustic sensor, however, have a software barrier implemented, eliminating access to audio services. For example, AXIS OS has no audio streaming APIs for the acoustic sensor. This means that neither users nor applications can initiate streaming or storing of audio. The camera's web interface has no audio streaming or storage options, and it also isn't possible to access audio services from a VMS or any other system where you have onboarded the camera.

AXIS OS is protected by several cybersecurity features enabled by Axis Edge Vault. The feature signed OS, for example, protects the device from software tampering. Only software signed by Axis can be installed and it isn't possible to replace it with other software.

Furthermore, cameras with an acoustic sensor run software version AXIS OS 12.0 or later, in which root access has been removed. This means that it isn't possible for users or applications to access audio streams through, for example, manual recording via ssh. For more information about root access removal and other cybersecurity measures in AXIS OS, see *AXIS OS Portal*.

The software barrier makes the acoustic sensor a more privacy-friendly solution for audio monitoring. It enables audio analysis without storing sensitive audio information linked to personal data.

5 Disclaimer

Please be advised that this document is provided "as is" without warranty of any kind for information purposes only. The information provided in this document does not, and is not intended to, constitute legal advice. This document is not intended to, and shall not, create any legal obligation for Axis Communications AB and/or any of its affiliates. Axis Communications AB's and/or any of its affiliates' obligations in relation to any Axis products are subject exclusively to terms and conditions of agreement between Axis and the entity that purchased such products directly from Axis. FOR THE AVOIDANCE OF DOUBT, THE ENTIRE RISK AS TO THE USE, RESULTS AND PERFORMANCE OF THIS DOCUMENT IS ASSUMED BY THE USER OF THE DOCUMENT AND AXIS DISCLAIMS AND EXCLUDES, TO THE MAXIMUM EXTENT PERMITTED BY LAW, ALL WARRANTIES, WHETHER

STATUTORY, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT AND PRODUCT LIABILITY, OR ANY WARRANTY ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE WITH RESPECT TO THIS DOCUMENT.

T10214032/EN/M1.11/2505

About Axis Communications

Axis enables a smarter and safer world by improving security, safety, operational efficiency, and business intelligence. As a network technology company and industry leader, Axis offers video surveillance, access control, intercoms, and audio solutions. These are enhanced by intelligent analytics applications and supported by high-quality training.

Axis has around 5,000 dedicated employees in over 50 countries and collaborates with technology and system integration partners worldwide to deliver customer solutions. Axis was founded in 1984, and the headquarters are in Lund, Sweden.