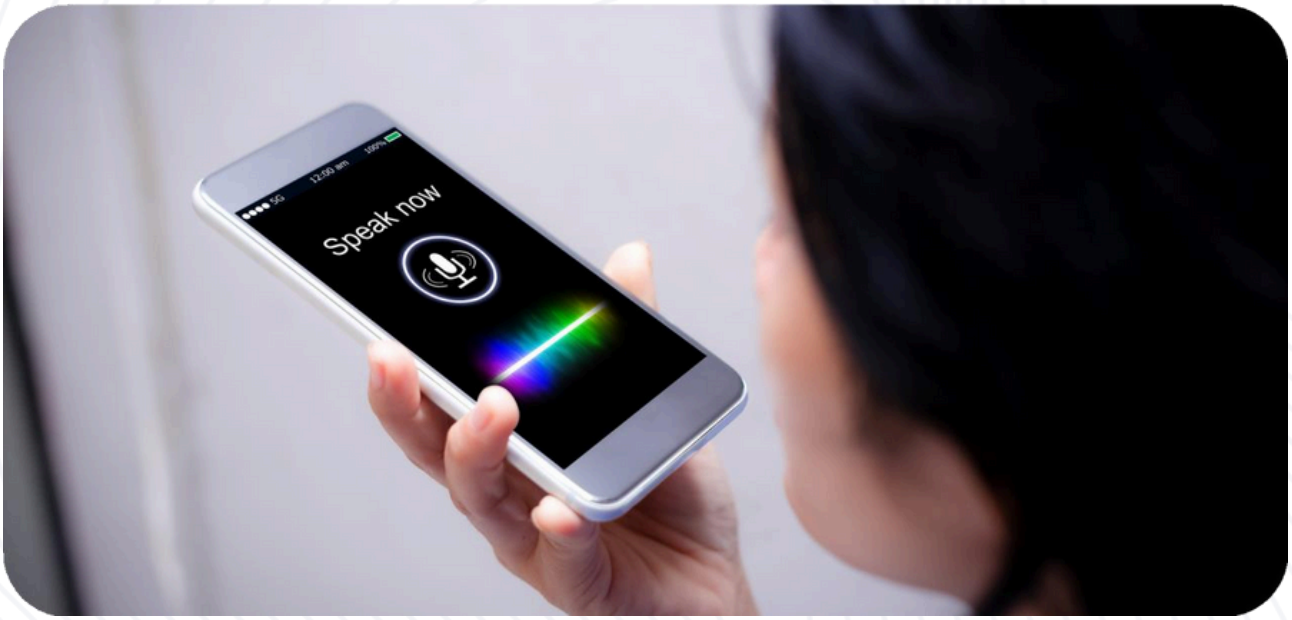
AURAYA

ArmorVox™

Product Sheet

ARMORVOX™

The next-generation voice biometric AI technology. Treat your customers with seamless and secure speaker recognition in any language on any platform.



According to IBM[1] , the average cost of a data breach is $3.92 million. Every organization, even the top 100 companies, is vulnerable to data breaches and other forms of cyber-attack. It is imperative to employ the best possible cybersecurity measures. Today, traditional security methods are insecure and inefficient, requiring far too many steps such as SMS tokens and email verifications. They fail to deliver satisfactory security and customer experiences. Remembering PINs and passwords can be frustrating and can be easily stolen, hacked and misused. Time is wasted conducting manual verification attempts and the prolonged agent handling times and jarred customer journeys of switching applications or devices can deter customers from using an organization's services.

KEY BENEFITS

THE NEXT GENERATION OF VOICE BIOMETRICS

Designed to deliver secure yet seamless customer journeys, ArmorVox™ is Auraya's advanced voice biometric AI technology that provides speaker recognition, and fraud prevention capabilities designed for fast, and intuitive experiences in all channels and languages

IMPROVED CUSTOMER EXPERIENCE

Customers often dread contacting customer support due to past negative experiences involving cumbersome identity verification processes. With ArmorVox, speaker recognition capabilities allow seamless and rapid identity verification. Customers can interact through IVR, chatbots, or web portals, enabling personalized self-service. If needed, agents can access the required data without manual verification steps, enhancing privacy and reducing frustration.

to

IMPROVED CYBERSECURITY

Many distinct voice characteristics are used to identify and verify a person. Physical characteristics such as the shape and size of a person's vocal tract and behavioral characteristics such as accent speed of speech, cadence, pronunciation, and emphasis are all accounted for when capturing voiceprints. ArmorVox takes advantage of these characteristics to generate highly secure and unique voiceprints which are then encrypted and cannot be reverse-engineered. Captured voice recordings and encrypted voiceprints do not leave the organization's secure infrastructure. Not even Auraya will be able to access the data. ArmorVox leverages its patented features to ensure accuracy and security performance. These features ensure that the best possible quality of voiceprint is captured and allow customization of security thresholds to ensure the desired level of security is set for each individual and each transaction, all while protecting users from fraudulent attempts such as using computer-generated voices, recorded voices, or even twin voice attacks.

REDUCING COSTS

Biometrically verifying customers in a self-service platform means that customers are served more timely and efficiently. For services that require a live agent, whether it's a service provider in contact centers, a chatbot, or a messaging app, having customers verified before reaching the agent allows for improved efficiency and reduced agent handling times as there is no need for manual verifications. ArmorVox also helps to reduce operational costs. In addition to reducing the cost of manual verifications. there is no longer any need for additional security services such as SMS charges or RSA tokens. The whole experience is seamless and frictionless, all the while maintaining regulatory compliance such as Know Your Customers (KYC) and Anti-Money Laundering (AML) HIPAA, GDPR, and the various privacy regulations in different jurisdictions.

KEY CAPABILITIES

VOICE ENROLMENT

ArmorVox can enroll multiple voiceprints for each user through text-dependent same-phrase, text-dependent unique-phrase, text-independent, text-prompted, or digit-independent tokens. These voiceprints allow verifications with as little as 2 seconds of net speech. Some text-dependent verifications can be as short as 1 second of net speech. Additionally, ArmorVox is compatible with any language, so users can enroll their voiceprints in their language.

Voiceprints are created by extracting acoustic parameters from a .wav file containing the spoken information. This .wav file can be sent from a digital device such as a computer or a tablet or collected from a conversation with an agent in a contact center or with a chatbot in a browser. After successful extraction, the original voice recording can either be deleted or stored in a secure archive. The voiceprint is encrypted and stored in a database under the control of the organization. From here, the voiceprint will be used when verifying or identifying speakers in the future.

VOICE VERIFICATION

ArmorVox requests users to provide some identification such as calling line identification (CLI or ANI), or a spoken customer number, or phone number, or account identifier, or the IP address of the digital device that they are using. A voice sample is captured when they say the identification information and then matched with the enrolled voiceprint in the database. If the voiceprint match passes the security threshold then the person can proceed as ‘verified’.

A voice sample can be captured and matched with a group of existing voiceprints in the database to produce a score. Using the score, the speaker’s identity can be determined. Obtaining extra information such as device ID or account number can be used to further confirm their identity

MULTI-PLATFORM COMPATIBILITY

Organizations can integrate ArmorVox into any cloud-based or on-premise platform, provided that the platform can post an audio .wav file to the ArmorVox server to conduct voice biometric processes.

ArmorVox can be integrated into on-premise legacy contact centers and even cloud-based contact centers such as Amazon Connect, Twilio, Five9, Avaya, Genesys, and so on. It can also be integrated into other digital platforms such as an interactive chatbot, a messaging application, or even access online web portals. With ArmorVox, organizations use voiceprints to securely identify and verify customers and even internal staff on any platform desired, providing a complete voice biometric experience for both organizations and their customers.

FRAUD PREVENTION

ArmorVox helps prevent fraud in real-time. ArmorVox can crossmatch over 125 million voiceprints per hour on a single server to check for potential duplicate voiceprint enrolments. The duplicate enrolments can be screened to check for fraudulent activity. This process can be used to identify fraudsters and add their voiceprint to a 'Suspected Fraudster' list. This list can be updated with voiceprints created from the historical recordings of calls that were later found to be fraudsters.

ArmorVox's fused active and passive modes allow a combination of digit-independent and text-dependent and text-independent voiceprints to be created from historical call recordings. These voiceprints can be added to the 'Suspected Fraudster List' and used to detect fraudsters attacking the organization in the future.

Additionally, Playback Protection combats recorded voices by requesting random digit or text-dependent challenges. Synthetic Voice Protection combats generated or modified voices through machine learning algorithms and synthetic voice artifact detection.

KEY FEATURES

TUNED UBM

With ArmorVox's built-in machine learning algorithms, the core models of the engine are automatically tuned to generate optimal results. This feature is capable of reducing the False Reject Rate by over 50%, where the prior initial success rate is already at a highly effective level.

ACTIVE LEARNING

Speakers may sound a little different each time they attempt a verification due to behavior patterns or devices used. With Active Learning, ArmorVox continually adapts and learns from past interactions. This greatly improves the quality of their voiceprint, ensuring higher success rates and increased accuracy. After three active learning cycles, this feature is capable of reducing the False Reject Rate by over 90%, where the prior initial success rate is already at a highly effective level.

SPEAKER-SPECIFIC THRESHOLDS AND SPEAKER-SPECIFIC BACKGROUND MODELS

When creating voiceprints, ArmorVox uses a patented process to create a Speaker-Specific Background Model and Speaker-Specific Threshold which improves the security performance for each individual. This allows ArmorVox to set levels of security for each voiceprint to meet the desired security outcomes required by the organization.

This patented feature ensures that every user in the system achieves the specified security outcome, rather than having a system-wide general threshold which may lead to discrepancies in security levels between speakers. This feature improves customer experience and security performance by reducing the False Reject Rate by a further 60% whilst maintaining the specified False Accept Rate consistent for every individual voiceprint.

CROSS-CHANNEL

Auraya's patented process enables users to enroll their voiceprint and verify their identity on any digital channel such as enrolling from a secure mobile app or web portal and using the voiceprint for verification purposes on any other channel such as in the contact center IVR, agent conversation or digital chatbot. ArmorVox can be deployed in on-premise or cloud-based solutions, whether it is a legacy telephony solution or on cloud-based platforms such as Amazon Connect. Additionally, with Auraya's patented HTML5-compliant browser-based voice enrolment and verification processes, users can interact with voice biometrics anywhere via a browser on their smartphones or computers

RAPID CROSS-MATCHING

In addition to enhanced security and convenient user experience, ArmorVox can provide real-time fraud detection background tasks such as impostor mapping and duplicate spotting. This means that ArmorVox can post immediate feedback if the user who is being enrolled in that specific instance is a known fraudster or someone who is already enrolled but under a different identity. ArmorVox achieves this through its fast cross- matching speed of over 125 million voiceprints cross-matched per hour on a single server. Moreover, the speed is dependent on the CPU of the server being used. If an organization requires a faster cross-matching speed to accommodate a larger activity, it can simply increase the number of servers.

FUSED ACTIVE AND PASSIVE MODES

With ArmorVox, organizations can use either text-dependent same-phrase, text-dependent unique-phrase, text-independent, text-prompted, or digit-independent voiceprint tokens for enrolling and verifying their users. Additionally, organizations can also use a combination of tokens to deliver faster verification. With this feature, organizations can use phone numbers, customer account numbers, employee numbers, and other identifiers to enroll and verify their users as well as implement random phrases or digits as a way to protect against fraudulent attacks.

UNMATCHED EFFICIENCY

ArmorVox enhances operational efficiency with faster onboarding and system calibration. Organizations benefit from seamless voiceprint enrollment and improved performance, minimizing delays and ensuring a superior user experience.

NEXT-LEVEL SECURITY

Advanced machine learning algorithms in ArmorVox detect and counter deepfakes and synthetic voice attacks. Enhanced cybersecurity protocols ensure that sensitive data remains protected against evolving threats.

SIMPLIFIED MANAGEMENT

The upgraded admin console simplifies system management, providing an intuitive interface for voiceprint administration and performance monitoring. Organizations can streamline operations and focus on delivering exceptional customer service.

RAPID CROSS-MATCHING

In addition to enhanced security and convenient user experience, ArmorVox can provide real-time fraud detection background tasks such as impostor mapping and duplicate spotting. This means that ArmorVox can post immediate feedback if the user who is being enrolled in that specific instance is a known fraudster or someone who is already enrolled but under a different identity. ArmorVox achieves this through its fast cross- matching speed of over 125 million voiceprints cross-matched per hour on a single server. Moreover, the speed is dependent on the CPU of the server being used. If an organization requires a faster cross-matching speed to accommodate a larger activity, it can simply increase the number of servers.

FUSED ACTIVE AND PASSIVE MODES

With ArmorVox, organizations can use either text-dependent same-phrase, text-dependent unique-phrase, text-independent, text-prompted, or digit-independent voiceprint tokens for enrolling and verifying their users. Additionally, organizations can also use a combination of tokens to deliver faster verification. With this feature, organizations can use phone numbers, customer account numbers, employee numbers, and other identifiers to enroll and verify their users as well as implement random phrases or digits as a way to protect against fraudulent attacks.

FLEXIBILITY AT ITS CORE

ArmorVox offers backward compatibility and supports multi-tenancy, allowing organizations to manage multiple environments with ease. Its adaptable architecture accommodates various deployment models, including on-premise, cloud, and hybrid solutions.

SEAMLESS TRANSITION

Organizations can migrate existing voiceprints from legacy systems like Nuance into ArmorVox without service disruptions. This ensures data continuity and enables quick adoption of the latest features.

BUILT FOR GROWTH

ArmorVox's scalable infrastructure supports increasing volumes of data and user activity while maintaining top-tier performance. It enables businesses to grow confidently, delivering secure and efficient services as demands evolve.

PLAYBACK PROTECTION

ArmorVox combats playback attacks by requiring the user to say a new random set of digits during the verification process. Unless the fraudster is presented with the same set of digits that directly matches the one that the fraudster has recorded previously, then the playback attack will fail all the time. If organizations are concerned about fraudsters recording each digit and playing it separately from a keyboard, then the organization can implement random phrase detection instead.

SYNTHETIC VOICE PROTECTION

Sophisticated synthetic voice generators can be detected using ArmorVox's model detect functionality. ArmorVox can be used to enroll a sample set of voices from these sophisticated synthetic voice generators. This model can then detect the specific artifacts that the synthetic voice generator has in any variation of the voices that are created from that generator. These models can then be added to the organization's fraudster list, where ArmorVox can crossmatch any future attempts to detect synthetic voices.

EASY DEPLOYMENT

Integrating ArmorVox into your existing on-premise or cloud-based solutions is easy. You can do it yourself or use one of your trusted technology partners.

---

[1] IBM. (2019). 2019 Cost of a Data Breach Report. Retrieved from

https://www.ibm.com/security/data-breach

Auraya Systems Pty. Ltd.

Auraya is a voice intelligence company with the mission of empowering people and organizations to interact and engage with convenience and security in all channels and languages. Auraya develops next-gen voice biometric AI technology to deliver easy-to-use and highly secure speaker recognition and fraud detection capabilities. Auraya provides its technology to a global network of partners who incorporate Auraya's voice biometric technology into their secure, customer-facing applications and fraud detection solutions. The ecosystem of partners delivers solutions in all industries including government, education, healthcare, financial services, retail services, and telecommunications. If you would like to talk to the team at Auraya, send us an email at info@aurayasystems.co

AURAYA

394 Lane Cove Road, Macquarie Park, NSW 2113, Australia

info@aurayasystems.com

aurayasystems.com

Australia | United Kingdom and Europe | Americas | New Zealand | Asia