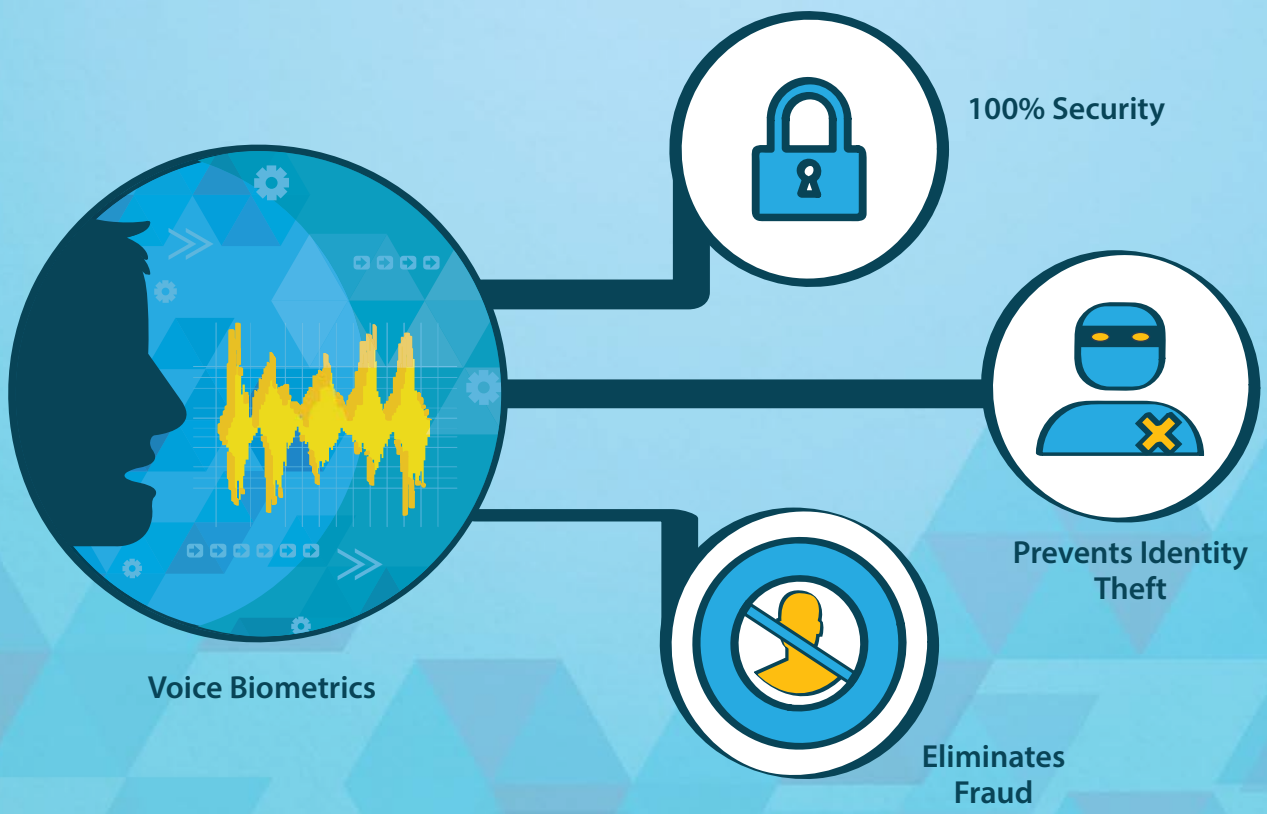
FREQUENTLY ASKED QUESTIONS ON VOICE BIOMETRICS

SUMMARY

Voice Biometrics authentication is the next level of security for the enterprises. Enterprises are implementing voice biometrics as a security measure to authenticate customers to access their systems. Voice biometrics has proved to be more secure than PINs, Passwords and Security questions.

Uniphore Software Systems, a pioneer in providing voice-based mobility solutions has integrated its Voice Biometrics solutions for many enterprises to eliminate fraud and identity theft. This white paper outlines the frequently asked questions related to voice biometrics, its credibility, enrollment, sample use cases, and more to give a fair understanding on integrating voice biometrics in enterprises.



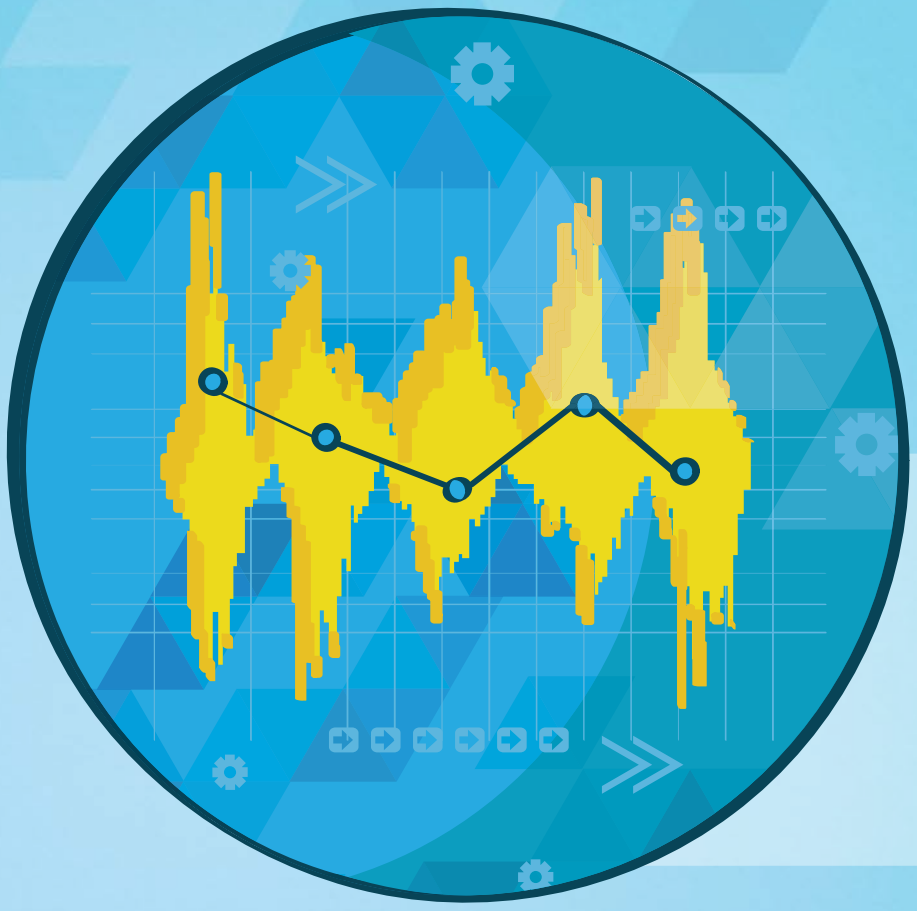
uniphore
Speech-based Mobility Solutions

TABLE OF CONTENTS

GET STARTED WITH VOICE BIOMETRICS

What is voice print?

Each time we speak, we reveal the unique physical and behavioral characteristics of our voice in the same way that our fingers leave fingerprints when we touch an object. When a voice is captured by voice biometrics software, a voiceprint can be collected to later identify the individual who spoke.



What is Voice Biometrics?

Voice Biometrics is a statistical model, just like any other biometrics technology, with a set of algorithms that analyze hundreds of speech characteristics, which fall into two distinct categories, behavioral and physical. The combination of all of these factors then produce a unique voice pattern for every individual called a voiceprint. The voice biometric software then compares the speaker's utterance to a voiceprint and produces a confidence rating that the utterance and voiceprint belong to the same speaker. In this respect, voice biometrics is very different from other biometric technologies, in that it is not only identifying physical traits, but behavioral traits as well. This technology is increasingly being adopted by organizations around the globe that include financial institutions, telecommunication services providers and other enterprises that require validating to identify customers within customer care channels.

How does Voice Biometrics work?

Voice Biometric authentication is comprised of two steps:

1) Enrollment – when we create the voiceprint

2) Verification/Identification

During enrollment of new speakers, the identifiers, also known as features, are extracted from several voice samples and are used to create a voice template, or voiceprint, which is stored in the system's database. The voice template describes the distribution of the features, but does not contain actual voice samples.

There are two types of speaker recognition, both of which can be used for authentication:

- ***Verification***
- ***Identification***

Verification is a one to one comparison that verifies an individual who he or she claims to be. An utterance is compared to the voiceprint of the claimed identity, and the speaker is either rejected or accepted.

Identification is a one-to-many comparison that identifies the individual from a set of individuals. In essence, identification is the process of identifying which speaker is speaking. An utterance is compared to a set of voiceprints, and the speaker is either identified or not. In case a speaker is not identified, he is defined as unknown.

What is the biometrics terminology used to measure the accuracy of voice biometrics?

The two biometrics terminologies used to measure the accuracy of voice biometrics are: **False acceptance (FA), False Reject (FR) and Equal Error Rate (EER).**

FA is the rate, generally stated as a percentage, at which imposters are accepted as authentic enrolled persons by a biometric system. This is usually considered to be the most important error for a biometric access control system. False acceptance means that users are accepted when they should not be. Security rate is the complementary number to the FA. e.g., if the FA rate is 0.4% then the security rate is 100%-0.4% = 99.6%.

FR is the percent of authentic speakers who were rejected. Automation rate is the complementary number to the FR. e.g., If the FR rate is 4.3% then the automation rate is 100%-4.3% = 95.7%

So, in a typical deployment, the voice biometric system needs to be tuned and thresholds set so as to balance between security and convenience.

The value of the point at which the false acceptance and false rejection rates are equal is referred to as Equal Error Rate (EER). When benchmarking systems, EER is the measure of the accuracy of the system. The lower EER, the better the system is performing.

MULTI-FACTOR AUTHENTICATION METHODS

What are the different authentication methods being used?

There are a number of biometrics from which to choose, ranging from

- *Fingerprints*
- *Hand Geometry*
- *Retina*
- *Iris*
- *Face*
- *Signature*
- *Voice*

Each biometric has both strengths and weakness.

Why offer Voice Biometrics to your patrons?

Voice Biometrics has a number of advantages:

- *It is the only biometric that allows users to authenticate remotely without the need of dedicated devices. A simple telephone or microphone is all that a user needs in order to authenticate using his or her voice. This lowers the cost of implementation.*
- *Voice biometrics' applicability across multiple communication channels such as cellular phones, broadens implementation opportunities.*
- *Voice biometrics is non intrusive and therefore it is easily accepted by the users.*
- *The low percentage of failures to enroll, when compared to other biometric technologies.*
- *Voiceprints require little storage space, allowing the systems to use standard computer equipment.*

How does Voice Biometrics differ from conventional authentication methods?

The comparison table below shows the advantage of voice biometrics than other authentication methods:

Attributes/Methods	Voice	Fingerprint	Iris	Face
Cost of Ownership	Lower	Higher	Higher	Higher
Equipment at Access point	No	Yes	Yes	Yes
Remote Identification Possible	Yes	No	No	No
Secure	Yes	Yes	Yes	Yes
Physically Intrusive	No	Yes	Very	Very
Possible to lose for forget	No	No	No	No

CREDIBILITY

What is the accuracy rate?

Uniphore's voice biometrics solution has proved accuracy consistently recording 0% FA (False Acceptance) and 3-4% FR (False Rejection) which is better than RSA global standards. It implies that no instances occurred where imposters break through the system.

What are the scenarios in which voice biometrics will not work?

Uniphore's voice biometrics solution has proved accuracy consistently recording 0% FA (False Acceptance) and 3-4% FR (False Rejection) which is better than RSA global standards. It implies that no instances occurred where imposters break through the system.

Can Voice Biometrics serve as a Unified Credential?

A person's voiceprint, once it has been registered via an application (e.g. the mobile application), can then be used to identify the same person in another application (e.g. the IVR). As such, voice biometrics can unify the often disjointed approaches to authentication that currently exist within internal and external systems. Instead of asking for a PIN in the IVR and a complex alpha-numeric password in the mobile application, the same passphrase "At ABC Company, my voice is my password" can be used to authenticate in both applications. This has helped organizations make the authentication experience consistent for customers, whilst complying with security requirements.

" A person's voiceprint, once it has been registered via an application (e.g. the mobile application), can then be used to identify the same person in another application "

Is it approved by international regulations/laws to use voice biometrics in user authentication?

The adoption of voice biometrics - regulatory:

- *The FFIEC (Federal Financial Institutions Examination Council) specifically mentions biometrics as an accepted method for authenticating customers and lists voice biometrics as one of the types used in two-factor authentication*
- *Satisfies FFIEC and FCC CPNI compliance and HIPPA/CMS guidelines; and is recognized by the FDA as a legally binding, E-Sign Act compliant, e-signature.*
- *BASEL report for Biometric Technology says 'voice scans' as one of the Endorsements from Regulators of the biometric authentication methods.*
- *The IT Act of 2008 validated the used of Voice as supportive evidence in a court of law*
- *MPFI minutes Resolution 7 –In India, you can use voice print as means of authentication for value below 1 lakh of mobile transactions (make the section of the minutes float here)*
- *In India at Chandigarh Forensic Science laboratories voice identification techniques are regularly conducted and the Supreme Court has held that voice identification data is admissible in court.*

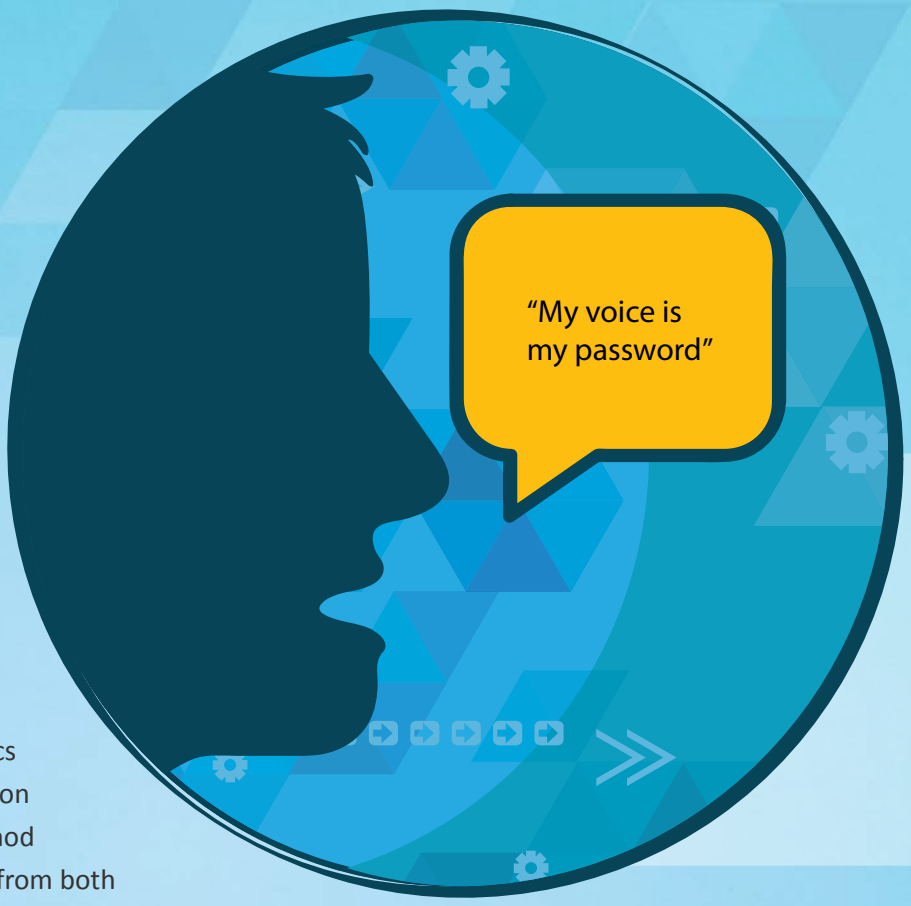
ENROLLMENT

What are the ways to enroll Voice Biometrics in an organization?

There are 4 ways in which Voice Biometrics is widely used across organizations:

- ***IVR Automated Authentication***
- ***Agent Assisted Authentication***
- ***Mobile Application Authentication***
- ***Employee Authentication***

IVR Automated Authentication



By far the most common voice biometrics application within organizations is the authentication of customers as they dial into the Interactive Voice Response (IVR) system. Typically, customers will be asked to speak a common passphrase, such as "At ABC Company, my voice is my password". Once authenticated, the customer can perform transactions or retrieve information on their account. If the customer chooses to transfer to an agent, they are already authenticated via voice biometrics and the agent can immediately service the customer. There is no additional need for an agent enforced interrogation process.

One of the main reasons why voice biometrics has been so prevalent in the IVR authentication space, is that the typical authentication method (PINs) is such a poor authentication method from both a security perspective (many people select PINs that are easily compromised) and from a user-convenience perspective (many people forget their IVR PINs as they do not call regularly). The return on investment is typically significant, as successful automated authentication with PINs is generally low (often in the 30% to 60% range) and fraud committed in the Call Centre is typically higher than in other customer care channels. As such, voice biometrics can significantly improve the customer experience by making authentication simple, reduce Call Centre costs by keeping callers in the IVR and increasing self-service rates, and by reducing fraud losses via making it more difficult for a fraudster to compromise an account.

Voice biometrics is utilized today within a wide range of IVR systems, including self-service wire transfer IVRs where voice biometrics secures multi–million dollar wire transfers to telecom services, IVRs where voice biometrics facilitates access to account settings and information.

Agent Assisted Authentication

Closely related to IVR authentication is the automated authentication of callers when they speak to an agent. In situations where authenticating callers in the IVR is not possible, or desirable, voice biometrics can be used when the caller reaches an agent. However, unlike authentication within the IVR, the caller is not required to speak anything specific to get authenticated. In these scenarios, voice biometrics is operating in a passive mode, listening to a live conversation with an agent and then providing the agent with a confirmation of identity on the agent's computer screen. This form of voice biometric authentication has the benefit of reducing the call handle time as the agent does not need to ask the customer a series of security questions before servicing the customer. Voice biometrics can also significantly reduce fraud as the Call Centre is particularly vulnerable to social engineering and other malicious attacks.

Although the use of voice biometrics by organizations in live agent calls has a less immediate financial impact when compared to automating authentication in the IVR, the implementation of passive voice biometrics is much quicker and requires no effort on the part of the customer. This is becoming increasingly appealing to organizations wishing to deploy voice biometrics to their premium customer segments. For these organizations, delivering an exceptional customer care experience provides the organization with a meaningful competitive advantage that can be measured in customer retention and new customer acquisition metrics. The level of personalization that can be delivered thanks to voice biometrics is comparable to establishing a personal relationship with the customer. For example, agents can answer calls, greeting a customer by name and immediately servicing their request. The customer feels as if the agent knows who they are and that they are valued by the organization. The agent treats the customer without any suspicion of identity and the threat of a fraudster representing as the customer is diminished.

Mobile Application Authentication

Beyond the Call Centre, the most significant area of growth for voice biometrics applications within organizations is the authentication of users via mobile applications. Currently, mobile application developers struggle with a basic trade-off. As authentication is made more secure, e.g. by implementing complex alpha-numeric passwords, mobile application usage drops. Typing combinations of numbers, letters and special characters is frustrating and leads to a high failure rate on a SmartPhone device. Initially, the alternative was to implement very weak authentication methods such as a 4-digit PIN or no authentication at all. This limits the functionality that can be offered within the mobile application. Voice Biometrics offers organizations with an elegant solution that favors usage whilst enhancing security. Similarly as within the IVR, SmartPhone application users can be asked to speak a common passphrase such as “At ABC Company, my voice is my password” to access the application or to authorize a high-risk transaction.

Voice Biometrics has allowed organizations to increase their mobile application usage and increase the number and type of transactions that can be performed on a SmartPhone device. This in turn reduces the load on more costly customer care channels, such as the Call Center.

Employee Authentication

Authenticating customers is the most common use-case for voice biometrics as a customer-facing solution, but the same technology can also be used to authenticate employees. Many organizations have successfully leveraged the technology for numerous internal applications. For example, voice biometrics has proven to be an effective method of automating the process of re-setting an employee's Windows passwords, authenticating employee-to-employee calls, and validating employee identity when dialing an internal Call Centre (such as the IT or the HR helpdesk). Increasingly, organizations are also using voice biometrics to secure highrisk transactions performed by employees and authenticating remote employees to work securely within applications.

Although the scale of these deployments is often smaller than the customer-facing applications, organizations can realize significant productivity gains by streamlining the authentication procedures and at the same time reduce internal fraud.

What are the industries that can use voice biometrics?

Voice Biometrics has been used across different verticals of the enterprise customers including

- *Telecom*
- *Financial/Banking*
- *Agriculture*
- *Healthcare*

SAMPLE USE CASES

How can we deploy voice biometrics in banks?

Voice Biometrics is effectively used in banks in some of the following key areas:

- *Customer Onboarding*
- *Automated outbound communication – customer alerts*
- *Automated Inbound communication – call center automation*

Using Voice Biometrics as an authentication mode, Banks can achieve:

INCREASED SECURITY:

- *Reduces identity theft by a factor of up to 200 – hence reducing payouts from the organization*
- *Liveliness detection and playback detection prevent malicious users from bypassing verification using an audio recording*

ENHANCED CUSTOMER SATISFACTION:

- *Easier and faster for customers to gain access to secure services by way of mobile apps, telephone and Web channels*
- *Better customer experience and boosts their confidence of telephone transactions*

REDUCED CUSTOMER CARE COSTS

- *Reduces agent handling time through increased automation*
- *Verification process can be reduced to a mere 5 seconds*

uniphore
Speech-based Mobility Solutions

How is voice biometrics used in the contact center?

In the contact center, voice biometrics is used primarily for secure access to information or assets. A speaker verification solution is based on a voice print provided by a user when enrolling. The speaker verification system stores the voice print in the system database. Later, when the customer calls in to request access, the system compares the caller's voice to the print on the file. If it is unclear, it may ask for additional information, or it may route the caller to a liver customer service agent.

Speaker verification is a natural fit for phone-based applications via the contact center because the system can be seamlessly integrated into the existing self-service experience of the caller.

DIFFERENTIATORS

Why Uniphore, if I can buy it from Nuance?

The key reasons to engage with Uniphore:

- *Pioneer in Multi-lingual Speech Recognition and Voice Biometrics solutions on Cloud*
- *Easy integration with IVR and mobile applications*
- *Support 20 languages and 100+ dialects across geographies*
- *Uniquely positioned to cater to the untapped opportunity to serve 6.7 billion global mobile subscribers, 72% of whom don't use smartphones.*
- *Global leader in providing commercially used Voice Biometrics platform used for Banking and Payment Transactions.*

The key differentiators of Uniphore's solution from Nuance product are:

- *Customizable as per client's requirements*
- *Multi-lingual speech recognition support*
- *Consistently recording 0% FA (False Acceptance) and 3-4% FR (False Rejection): better than RSA global standards*
- *Compliant with Global Mobile Banking Guidelines*

> "Uniphore uniquely positioned itself to cater to the untapped opportunity to serve 6.7 billion global mobile subscribers, 72% of whom don't use smartphones "

uniphore
Speech-based Mobility Solutions

What are the languages your voice biometrics solution supports?

Currently Uniphore's voice biometrics solution recognizes 20 global languages including English, French, Hindi, Swahili, Arabic, Filipino, etc. and supports 100+ dialects.

Who are your voice biometrics solution buyers?

Uniphore is offering its voice biometrics solution to over 100 large enterprise customers and 3 million end users. Customer case studies and details can be shared upon request.

EXPERIENCE

How many years you are providing this solution to customers?

Uniphore is a pioneer in providing Multi-lingual Speech Recognition and Voice Biometrics solutions on a Cloud. Uniphore is offering this service to many enterprises for the past 6 years with proven track record on increasing the ROI and efficiency in the customer's operations.

How many times your customers reported voice biometrics failure? and How did you overcome those situations?

The FA (False Acceptance) reported by customer is 0%. There is no single instance of an unauthorized person being authorized by the system. FR (False Rejections) is around 3-5% which is due to noisy ambience or training related issues.

By including appropriate help messages in case of failure, we were able to overcome the issues. For example, if the person is speaking too soft, the system will ask the person to speak aloud.

USABILITY

How user-friendly are your solutions to end consumers?

Voice biometrics is much more user-friendly than any other biometric authentication. It can be integrated across multiple communication channels such as cellular phones, thus increasing the user acceptance rate. Another key reason for users to accept voice biometrics, it is non-intrusive and it is quite natural to speak rather than to put an eye up to a reader.

What if a caller has a cold?

The complexity of the human voice allows for analysis of a large quantity of data points. While one part of the vocal tract may be affected by a cold, the speaker verification engine can still accurately verify the caller's identity based on those parts of the vocal tract that are unaffected. Only extreme vocal change conditions, such as laryngitis will prevent the caller from successfully accessing the system.

Don't voices sound different with time of day, age or sickness? How can Voice Biometrics handle it?

Voice does change over time, but the speaker verification solutions are designed to handle those changes. To handle slow aging-related voice changes, the systems regularly update users' enrolled voice templates. Voice changes during the day, such as 'wake up voice', although noticeable to human ears, are ignored by the engines.

Can a caller use any telephone?

Our solution supports all telephone standards currently in use, Users may call from various telephones, mobile or landline, regardless of which type of phone they may have enrolled with.

How long does it take to enroll a caller?

Enrollment is an automated process which takes less than a minute. During the process, a caller is asked to repeat keywords 3-4 times. The system guides the user through the enrollment process and confirms successful completion.

Can a caller use different telephone numbers to verify his identity?

Our solution recognizes the voice print of the user; it doesn't have any implications on the user telephone number. However we can make telephone number as a first level of authentication attribute if required by the client.

Can background noise influence a system's ability to verify the user?

Our voice biometrics technology uses special filters that handle background noises, thus permitting analysis of the relevant voice signal. Background noises such as ambience noise, people talking, and road traffic are handled by the system.

RISK ASSESSMENT

Is voice biometrics more secure than PINs and passwords?

PINs and passwords are easily compromised through intentional theft, user apathy and even shoulder surfing. Voice cannot be stolen, compromised, or forgotten and hence it is highly secured than PINs and passwords.

Has voice biometrics been hacked before?

No. An independent study was also conducted on voice biometrics, which states that imposters were not able to hack the system. The case study and its results can be shared upon request.

How secure voice biometrics is against recording and playback attacks?

Voice biometrics solutions must ensure that the biometric sample is actually collected from the person being authenticated. This can be particularly challenging over a phone network where there is no way to see whether the caller on the other end of the phone line is actually speaking or is playing a high quality recording of another person's voice.

Speaker verification solutions from Uniphore prevent recording and playback attacks in several ways. First, it can identify characteristics of a recorded vs. live voice. Secondly, some systems deploy multi-factor authentication as part of the security strategy. This requires more than just the spoken voice, often combining knowledge authentication. e.g., something that a caller knows is being asked with speaker verification. Thirdly, Uniphore can implement a challenge-response method where the caller is instructed to repeat a short sequence of random phrases that could not have been pre-recorded.

What if my data gets leaked to the competitor who might be one of your customers too?

Our solutions will not use any public hosted infrastructure; all the deployments are carried out on an in-house infrastructure or on a private cloud. So there is no possibility of Uniphore making the data public.

IMPLEMENTATION

What is the typical ramp up period?

Usually voice biometrics is used as a part of a use case in any organization like say, attendance or customer verification during onboarding. While configuring voice biometrics takes around 2 weeks, and it also depends on the individual use case.

TRAINING AND SUPPORT

Will Uniphore give training on how to use voice biometrics and monitor the results?

In case of IVR applications, the voice prompts direct the user how to speak. In case of mobile or web applications, clear instructions will be provided in the mode of user manual. Uniphore will train the client and their representatives who can further train their end-customers.

ABOUT UNIPHORE

The ability to use speech to communicate is a primary reason for the evolutionary success of the human race. Uniphore's solutions extend this insight to the evolution of human-machine interaction. Uniphore's solutions allow any machine to understand and respond to natural human speech, thus enabling humans to use the most natural of communication modes, speech, to engage and instruct machines. Enterprises across industry, size and geographies deploy Uniphore's solution to dramatically improve employee productivity and deliver superior customer service.

As a leader of voice-based solutions, Uniphore has pioneered the development of mobile applications with the combined capabilities of Speech Recognition, Voice Biometrics, and Data. Uniphore boasts a roster of high-profile, satisfied customers across multiple verticals – Financial Service Providers (mobile commerce & banking), FMCGs & NBFCs (sales force automation), and Agriculture, Healthcare, & Education (content delivery services).

Since its inception in 2008, the company has grown at an exponential rate, and today it supports nearly half a million registered end users on its platforms every month. For more information on Uniphore visit www.uniphore.com.

Contact Us:

Uniphore Software Systems
India - +91 44 6646 9878
Dubai - +971 501528717
Philippines - +63 9278830228
Email: info@uniphore.com

uniphore
Speech-based Mobility Solutions