FROST & SULLIVAN

Improving Customer Journeys with Biometric Authentication Systems

Biometric Technologies Enhance the Customer Experience While Complying with the Highest Security Standards

Global Information & Communications Technologies Research Team
at Frost & Sullivan

The Growth Pipeline™ Company
Powering clients towards a future shaped by growth

MFE8-76
May 2021

Contents

Contents (continued)

Growth Opportunity Analysis—Biometric Authentication

Definitions

AI is a general class of technologies that seeks to emulate human cognitive capabilities and assist in decision making, with high accuracy and speed using data-driven intelligence and self-learning abilities. This set of technologies is diverse and encompasses a number of subsets.

Automatic Speech Recognition (ASR) is an independent, machine-based process of decoding and transcribing (word sequence) an utterance. ASR systems incorporate an acoustic model that determines the relationship between audio signals and phonetic units in a language, in addition to a language model that matches sounds to words and word sequences. Natural language processing (NLP) is the most demanded version of presently developed ASR technologies.

Biometrics Authentication is a user identification and verification process that uses unique physical and behavioral characteristics, such as fingerprint, iris, and palm vein.

Biometric Payment is a point-of-sale (POS) technology that relies on biometric authentication to identify and authorize the user for deducting funds from a bank account. Fingerprint payment, based on finger scanning, is the most common biometric payment method; however, facial recognition is gaining traction in this space.

Bots are computer programs built to engage with an individual and emulate humans using either web chat or speech interfaces. Bots range from a basic app that answers simple queries or seeks to entertain to fully conversational bots with intelligence embedded into the app and integrated with back-end systems.

Deep Learning (DL) is a machine learning (ML) technique that trains machines and software apps to understand and use algorithms that can unravel high-level abstractions in large volumes of data. DL can be considered as a multilevel ML architecture, in which several levels of ML are used to parse problems. DL is an approximation of a brain-like structure or neural network.

Facial Recognition is a biometric process of identifying and verifying a person by analyzing and comparing patterns based on facial contours. Face biometrics has garnered high popularity in the past two years.

Icon Source: Gettyimages.in

Source: Frost & Sullivan

Definitions (continued)

Fingerprint Recognition is a biometric process of electronically obtaining and storing human fingerprints for biometric authentication. This modality is the most widely used.

Iris Recognition uses mathematical pattern recognition techniques of one or both irises to identify people based on unique patterns within the region surrounding the pupil of the eye.

ML applies to a class of computing that allows machines to analyze data, learn, and predict outcomes. ML is a process by which a computer is trained to identify patterns in new inputs or data sets, based on the patterns it has been “taught” with prior data. Once trained, the ML system can be expected to find predictions reliably in subsequent data sets. ML applications can be self-trained, human trained, or a combination of both.

Multifactor Authentication (MFA) refers to a security system that uses more than one form of authentication, compared to the contrary method of single factor authentication that uses only the user ID and password. In many countries, second factor authentication(2FA) is a mandatory mode of authentication for banking.

NLP is the application of pattern recognition technologies to understand human language and can be applied to either text or voice channels. When applied to voice channels, complex front-end processing is required to parse speech into discrete words and then recognize those words. NLP typically front ends other AI applications, such as chatbots.

Natural Language Understanding (NLU) is a narrow subtopic of NLP that deals with machine reading comprehension. NLU refers to the process of teaching machines to comprehend and interpret what a text really means. Comprehension is the previous step to processing the information. NLP focuses on what is said, and NLU focuses on what is meant to be said.

Palm Vein recognition is a biometric identification process based on the unique patterns of veins in the palm of the hand.

Icon Source: Gettyimages.in

Source: Frost & Sullivan

Definitions (continued)

Voice ID is a biometric method of speaker recognition using vocal characteristics to identify users uniquely. This modality is commonly used for remote authentications.

Voiceprint is a set of measurable characteristics in the human voice that enables the unique identification of an individual. These characteristics are converted and expressed as a mathematical formula based on the physical configuration of the speaker's voice.

Icon Source: Gettyimages.in

Source: Frost & Sullivan

Evolutions of the Contact Center

Contact Channels

Traditional

- Phone
- SMS
- Email

Digital

- Mobile
- Video
- Social

New integrations, features and applications

Quality Management

- Measurement System Analysis (MSA)
- Standardized Processes
- On-Demand Quality Assurance Model
- Cybersecurity upgrades
- **Authentication upgrades**
- Compliance solutions

Workflow Optimization

- Robotic Process Automation (RPA)
- Intelligent Process Automation (IPA)
- Automated workflows
- Smart Knowledge Management
- First contact resolution (FCR)
- Flow Designer

Analytics

- Self-Service Analytics
- WFO Analytics
- Cross Channel Analytics
- Predictive Analytics
- Speech Analytics
- Text Analytics

Self-service

- Voicebots
- Smart IVR
- Chatbots

Workforce Optimization

- Upgraded Workforce Management Solution
- Upgraded Workforce Optimization Solution
- Introduction of WAHA models
- Gamification applications
- eLearning and Coaching
- Cobrowse

Augmented Intelligence

- VoC and Sentiment Analysis
- Assisted Chat
- Smart Routing
- Cognitive Knowledge Management

Enablers

Data Management
Unified Customer View/Business Intelligence/Data Quality and Governance

Technology
AI/Unified Agent Desktops/Conferencing and Collaboration/Cloud Computing

Source: Frost & Sullivan

Approaches to Authentication

User authentication enables a system or device to ensure that an entity is who it claims to be. This process has many uses, such as implementing access restrictions or monitoring the use of a service.

Authentication has many different scenarios, such as remote authentication through the web, remote authentication through other protocols, and authentication on a device (e.g., mobile phone, tablet, or computer). In addition, authentication has different methods, and the best choice depends on the authentication scenario. A method that is adequately useful and secure in one scenario might not be useful in another.

System Authentication Methods

- Biometrics: biometric authentication solutions to identify individuals through unique physiological and behavioral features using visual, audio, and behavioral data
- Credentials: username and associated password (traditional method of system authentication)
- Token-based authentication: based on something the user has, such as a code book or card, smart card, and public key infrustructure (PKI)-based certificates
- Alternative knowledge-based systems: alternatives to text-based passwords, such as graphical authentication systems or security questions
- Alternative device authentication: sending an SMS message or calling the user's phone

Three Main Approaches to Authentication

- Single-factor based on one method or input only
- Two-factor that adds one method or input to the process
- Multi-factor that relies on three or more data inputs

When looking to add or replace an authentication method, avoiding the need to replace a weak or inappropriate authentication method with another that is as bad or worse is essential.

Source: Frost & Sullivan

Biometric Authentication and the CX

- Biometric authentication solutions identify individuals through unique physiological and behavioral features using visual, audio, and behavioral data. The solutions can identify and analyze physical features, such as fingerprints, eyes, voice, scent, or DNA, to carry out reliable user authentication.
- Some of the most used biometric authentication technologies include fingerprint scans and voice or face recognition.
- End users demand improved security but not at the expense of a poorer CX. Security and risk management managers continue to search for technologies and mechanisms that will allow for secure, accurate, fast, and reliable identity corroboration processes.
- Vendors and developers endeavor to increase end users' trust in their apps while providing a higher quality CX. Passwords are becoming obsolete for businesses and end users alike. Passwords are difficult to remember, can be easily hacked, tend to make the authentication process longer, and increase the probability of breaches. In 2020, hacker attacks increased by three-fold in one year.
- Technology advancements, such as in biometrics, are helping organizations come up with more innovative business processes that can strike an adequate balance between security and CX simultaneously.
- Recent biometric technologies allow the enhancement of customer journeys while adhering to the highest security and compliance requirements.
- The adoption of biometric authentication solutions has been augmented as businesses look to deliver a CX that is secure, fast, frictionless, and personalized.
- Biometric authentication solutions can enhance the CX while reducing business costs, fraud, and authentication difficulties.

Source: Frost & Sullivan

Biometric Authentication and the CX (continued)

- Biometrics are transforming customer journeys and the way companies engage with their clients. Businesses are shifting to a biometric world, from using mobile devices that incorporate biometric authentication processes to replace pin codes to using biometric data to open an account.

Why are Biometrics Secure?

- Biometric authentication is dependent on the extreme difficulty of impersonating someone who presents unique biometric traits to a sensor.
- Well-built biometric authentication solutions do not really store an image or recording of a user's biometric traits (e.g., voice, eye, or fingerprint). Instead, these solutions register and store a mathematical representation or sample of the traits (also known as template).
- Even if people have similar traits, anything other than a user's actual registered trait should not authenticate the user.
- Some biometric authentication systems include liveness detection functionality, which identifies whether a presented biometric trait is from a live user or is digital or manufactured.

Source: Frost & Sullivan

Growth Environment—Evolution of Identity Authentication Techniques

1900s

Token-based System: Identity verification first required the presentation of physical hardware tokens, such as an identification card or physical access card, containing an individual's information. The relative ease of stealing tokens subjected organizations to significant risk.

1960s

Credentials: Creating identity credentials through partially unique passcodes, phrases, or PIN codes could eliminate the risk of the physical loss of an identity token; however, user behavior or coercion by a fraud perpetrator led to these credentials being ripe for theft or fraudulent use.

2000s

Physical Biometrics: Biometrics were widely introduced, where physical characteristics of an individual, such as fingerprint, facial geometry, iris pattern, and palm print, are used for authentication. Physical biometrics offer a modality that is physically tied to the individual, giving fraud perpetrators a much lower degree of success.

2020s

Behavioral Biometrics: The future of authentication involves uniquely measuring human activities and patterns based on an individual's operational actions, characteristics, and session behavior.

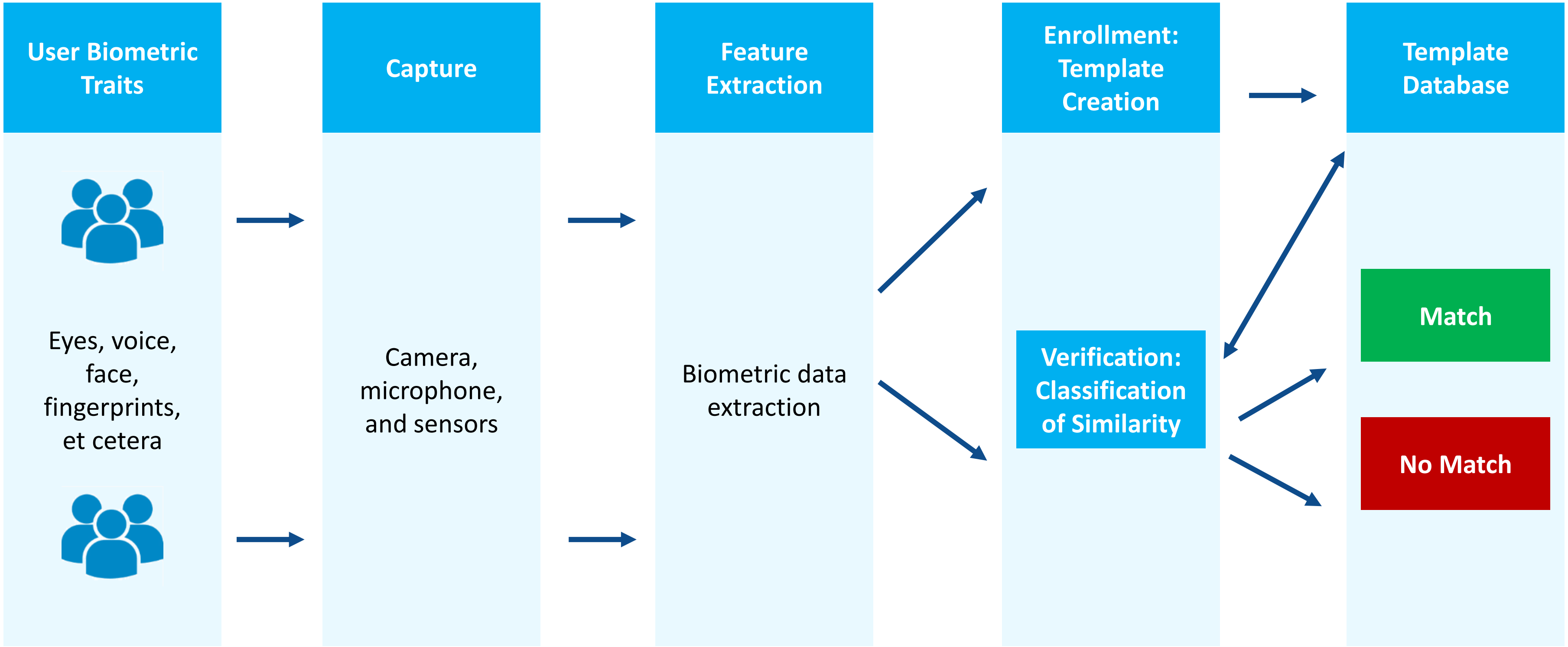
Source: Frost & Sullivan

How Do Biometric Systems Work?

Biometric Systems Have the Following 2 Modes:

- **Verification:** This mode determines whether a user is who he/she claims to be. The system validates the user's identity by matching the captured data with the template stored in the database.
- **Identification:** This mode determines the user's identity. The system identifies the user by searching all the templates in the database for a match.

Biometric Systems Data Workflow



User Biometric Traits
Eyes, voice, face, fingerprints, et cetera
Capture
Camera, microphone, and sensors
Feature Extraction
Biometric data extraction
Enrollment: Template Creation
Verification: Classification of Similarity
Template Database
Match
No Match

Source: Frost & Sullivan

Biometric Authentication Modalities

Physiological Biometrics

Physiological biometrics identify and verify a user based on human body traits, including fingerprints, face, or eye iris.

Modalities:

- Fingerprint recognition
- Hand geometry and vein recognition (palm or finger vein)
- Facial recognition
- Iris recognition
- Retinal identification
- Facial thermography and hand thermography
- DNA matching

Behavioral Biometrics

Behavioral biometrics methods identify and verify a user based on the user's actions when performing some tasks, such as handwriting, speaking, and typing.

Modalities:

- Voice verification
- Keystroke dynamics
- Handwritten signature
- Gait analysis
- Lip motion

With technology advances, many new biometric methods have emerged, and new companies have appeared in the market, thus opening up new opportunities, use cases, and applications for using biometric authentication systems. In addition to highly demanded fingerprint and facial recognition technologies, methods based on iris and retinal recognition and voice verification are gaining the most attention.

Automated fingerprint identification is the most widely used biometric authentication method today. Moreover, this method is widely used in offices where it is necessary to verify visitors reliably and is already integrated into almost every smartphone on the market.

Source: Frost & Sullivan

Key Metrics for Measuring Biometrics Technology

True Acceptance Rate (TAR) measures how well a biometric system accurately matches the biometric attribute from a subject with the available enrollment data from the same subject.

True Rejection Rate (TRR) measures incidents where the subject’s biometric attribute is accurately not matched against any other biometric data available in the database that does not belong to the subject under purview.

False Acceptance Rate (FAR) is the number of times the biometric template is incorrectly matched with a different biometric template in the database as a proportion of the total number of times it should have been rejected.

False Rejection Rate (FRR) is the number of times the biometric template is not matched with the correct biometric template in the database as a proportion of the total number of times it should have been accepted.

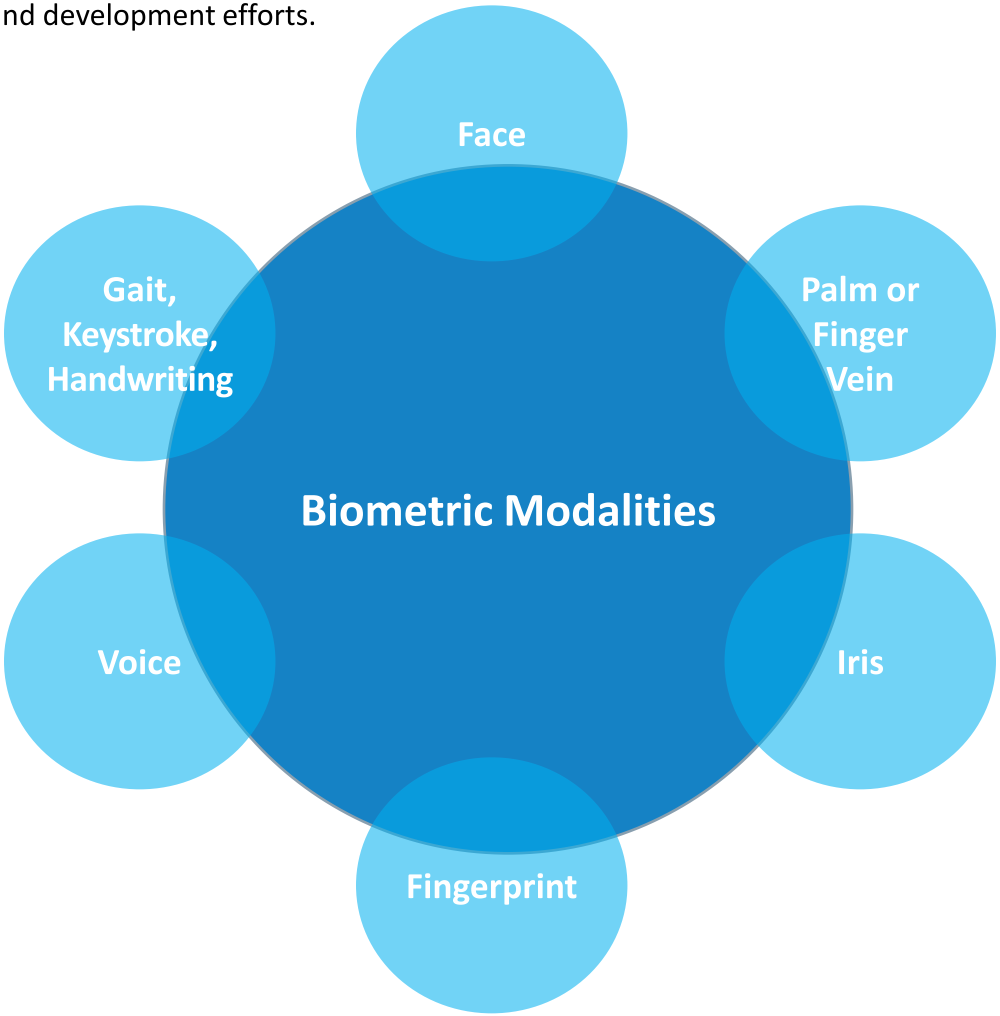
Icon Source: Gettyimages.in

Source: Frost & Sullivan

Biometric Modality Options in the CX Space

Selfie authentication has become popular as a result of refined technology and the persisting impact of COVID-19 (e.g., avoiding human touch). This modality is one of the fastest growing, in terms of use and development efforts.

While this modality is more often used in forensics and security-related issues than in the CX, innovative use cases will emerge over the next 15 years.



This modality continues to have a small share of biometric solutions and is particularly rare in the CX field.

To authenticate a user, detection capabilities include vocal inflection, syntax, word choice, and liveliness. Voice authentication is increasingly applied in the CX space.

During the pandemic, this modality has gained further traction and is becoming more widely used. New use cases in the CX space will emerge over the next 10 years.

Fingerprints remain the standard for biometric authentication and identity verification measures and are extensively used in smartphones.

Source: Frost & Sullivan

State of the Biometrics Market

High Demand for Biometric Technology

93% of users prefer biometrics to passwords.

92% of banks want to adopt biometric technology.

88% of bank executives expect to be a part of a discussion around biometrics technology.

The Major Driver is Dissatisfaction with Passwords and PINs:

- Over half of passwords are used at least twice.
- Twenty-one percent of users forget passwords after 14 days.
- Twenty-five percent of individuals forget at least one password every day.
- One-third of online transactions are abandoned because of forgotten passwords.

Source: Oxford University Department of Computer Sciences and Mastercard, 2017; Frost & Sullivan

Benefits of Biometric Authentication

Benefits
Biometric technologies assist in creating frictionless customer journeys.
Biometric technologies guarantee the rapid enrollment of employees, customers, or business partners.
Biometric tools are easy to use for user.
Biometric tools require negligible training as opposed to token-based or alternative authentication systems.
Biometric traits cannot be conjectured or stolen.
Biometrics can increase standardization across a broad set of mobile, desktop, and server devices.
Biometrics tools ensure high processing speed and are thus less time consuming for users.
Biometric traits cannot be misplaced or forgotten; therefore, they are convenient for users.
New biometric hardware and systems are continually being developed to improve the user experience.
Biometrics are non-transferrable because everyone has a unique set of biometrics features.
Biometrics provide quick scalability for large corporations or a large number of users.
These technologies ensure cost savings in the long run.
These tools provide high security and assurance.

Source: Frost & Sullivan

Limitations of Biometric Authentication

Limitations
Biometric databases can still be hacked.
Biometric solutions involve high development, setup, and implementation costs, especially for specific use cases or smaller outfits.
Biometric tools require an electrical current or battery to operate. If the device runs out of battery or there is an electrical problem or a blackout, the biometric tool will not operate.
False rejects and false accepts can still occur.
In case of a security breach, hackers have access to personal user data.
Some biometric devices can limit the privacy for users.
Regulations may limit the deployment or the use of some biometric methods.
Reparation of a broken or damaged biometric system generally requires the presence of professional teams.
Many external factors can affect the performance of a biometric system, such as environmental aspects, user behavior, physical disabilities, and badly maintained systems.
User organizations need certain previous knowledge or guidance to determine the most appropriate biometric method for their use case, which implies longer implementation processes.

Source: Frost & Sullivan

Biometric Authentication Use Cases in the CX Space

AI-powered biometric authentication tools can optimize customer journeys across many industries. Popular use cases include the following:

Access Control: Smart access systems allow organizations to grant permission based on organization membership and user context. Different types of user contexts include location (e.g., a specific province or country), device (e.g., device access control), user profile (e.g., group membership), and network (e.g., new IP and virtual network). Biometrics are commonly exploited in access control systems.

Financial Transactions: Biometric authentication technology is used to speed up financial transactions and prevent fraud. Banks and financial service businesses are using authentication technology for making high-value, contactless transactions (authenticating the cardholder); viewing account balances; and making deposits through a mobile app or at ATMs that can scan a user's fingerprint.

Identification for Benefits Cards: Holders of benefit cards (either social security or corporate) can share a PIN or a password with other people but cannot do the same with biometric data. Issuers can harness biometric tools to avoid fraud and ensure that only the real cardholder receives the card benefits.

Next-generation Customer Care: Voice recognition can identify and verify users and give self-service systems (e.g., chatbots, voicebots, and smart IVR) and contact center agents all the customer data they need to provide better service. Biometric authentication tools drive efficiency and minimize the time that virtual or live agents spend authenticating the user.

Onboarding Processes: Over 40% of new users abandon an onboarding process after 20 minutes, mainly because they are asked for an excessive amount of personal data and because of the length of time taken in the process. Automated processes through biometric authentication facilitate operational efficiencies and cost savings, adding value and enhancing the CX.

Icon Source: Gettyimages.in

Source: Frost & Sullivan

Biometric Authentication Use Cases in the CX Space (continued)

Additional popular use cases include the following:

Patient Identifier: Biometric authentication tools can help hospitals and other healthcare providers confirm a patient's identity and guarantee that caregivers have access to the correct clinical records and more.

Prevention of Identity Attacks: Multi-factor authentication systems and single sign-on solutions that incorporate biometric data can block suspicious login attempts to thwart threats, including phishing, ID stuffing, password spraying, and other types of takeover attacks.

Purchases: eCommerce websites and retailers use biometric authentication solutions (e.g., facial recognition) to power automatic checkout features. In the future, retailers will be able to capture the same data about shoppers in the store that they presently capture online, providing tailored engagements and personalized product offerings.

Self-checkin: Innovative airlines offer passengers the option to check in and board using facial recognition. Similarly, hotels and other hospitality companies are beginning to deploy self-checkin options using biometric authentication.

Icon Source: Gettyimages.in

Source: Frost & Sullivan

Key Trends Across Sectors

Biometrics will continue to grow sharply and steadily over the next 10 years, with AI and behavioral biometrics expected to complement the various physiological biometric technologies.

Financial Transactions

- Many financial institutions are upgrading their authentication strategies and looking into biometrics to replace the PIN/password and digital signatures in mobile transactions.
- The implementation of biometric technology for mobile transactions (facial and fingerprint recognition) will continue to grow.
- Additional implementations of biometric technology will provide users with improved levels of security and ease of operation.

eBanking

- With the increase in the use of smartphones, most banks have created native banking apps.
- Incorporating biometric technology in eBanking has improved customer loyalty.
- The added security delivered by biometrics (e.g., fingerprint, retina, iris, and face recognition) has been widely accepted by customers. Higher biometrics penetration in this segment is expected.

Contact Centers—Voice ID

- Voice biometric authentication reduces the average handle time (AHT) by eliminating the need for authentication questions asked by the agent.
- Voice biometrics can successfully battle fraud, particularly with a database of fraudsters' voiceprints.
- The adoption of voice biometrics in contact centers will grow at a fast pace.

Public Services

- Biometrics could aid in identifying citizen data and in preserving data integrity.
- Many countries are deploying biometrics technology in ePassports, which are travel documents that carry embedded personal and digital biometric data. ePassports increase the efficiency of administrative processes and improve the traveler's experience.
- For example, the Aadhaar program in India is the largest biometric database, with 1.2 billion records.

Retail

- Biometrics will make inroads in the future of retail payments.
- Fingerprint biometrics have been used for retail payments on a big scale. For example, Apple Pay and Apple Card involve pay-by-touch with a mobile phone.
- Amazon is testing a biometric solution that will allow customers to pay by using their palm in physical stores. The system would link a user's palm image to a payment card.

Source: Frost & Sullivan

Biometric Solutions—Decision-making Factors

End-user organizations should assess a series of factors when selecting a vendor.

Performance: The biometric solution should yield accurate results. Algorithms provided with hardware should detect and match with an existing database.

Cost: End-user organizations should understand the costs associated with these systems. Product pricing varies according to the type of biometric modality and use plan.

Interoperability: The high implementation cost of a biometric solution is a challenge if it lacks interoperability.

Customer References: Biometric implementations carry weight in terms of customer acquisition. Customer references provide an important competitive edge because they relate to a provider's experience in the field and brand name in the market.

User Friendliness: Organizations prefer turnkey solutions, and offering user-friendly products bodes well with end users. A wide array of product offerings from suppliers will be an added advantage.

Compliance: The solution and procedures must meet all compliance and regulations regarding possession and use of biometric data.

Channels: Solutions can be deployed across different channels, such as mobile, web, branch, call center, and wearable. Multichannel options provide a strong product differentiator.

Source: Frost & Sullivan

Key Deployment Considerations for End-user Organizations

When deploying biometric authentication tools, end-user organizations need to consider a series of issues that might affect solution performance and outcomes.

Data Sensitivity: Some data that authentication tools might capture is sensitive, making it necessary to assess the data management capabilities of existing systems and detect needed security improvements.

Pilot Implementation: Businesses should begin with small pilots to eliminate bugs, minimize risks, and ensure their efforts produce significant CX enhancements.

Centralized Data and Real-time Tracking: Businesses should record authorization and access logs in real time to register templates and enable early threat detection.

Data Storage: Business will need to consider where biometric data will be stored. Date security is critical when transferring users' data from biometric hardware to data centers.

Comprehensive Automation and Tech Plan: The implemetation of biometric tools should not be seen as an intrinsic plan in itself but as a central element of a larger automation and technology CX-related plan.

Ensure a Seamless and Secure CX: Authentication processes must ensure the CX is frictionless, personalized, and secure. Companies should determine the most adequate tools for their specific use case.

Source: Frost & Sullivan

Biometric Authentication Provider Profile

Biometric Authentication Provider Profile

This section profiles an innovative vendor to watch that makes exciting CX use cases possible.

Frost & Sullivan selected a vendor offering advanced AI-powered biometric modalities (e.g., voice).

Inclusion Criteria Comprised by the following:

- Provider offers biometrics capabilities.
- Provider offers an enterprise-class authentication solution.
- Provider has experience with CX use cases.

Source: Frost & Sullivan

Vendor Profile—Phonexia

- Phonexia offers an extensive set of innovative speech recognition and voice biometrics solutions to meet multiple business and governmental use cases and challenges. Phonexia's Voice Verify authenticates customers reliably based on their voice when they reach out to a contact center that uses Phonexia's proprietary voice biometrics technology.
- With Phonexia Voice Verify, customers can verify callers appropriately after only 3 seconds of net speech, with over 92% accuracy (based on the NIST SRE16 testset). The solution increases its accuracy as the conversation continues or after calibrating the system on the customer's data. Apart from the automated, voice-based authentication, the solution helps organizations meet several security regulations and shorten the authentication process of an average call by over 30 seconds, greatly decreasing customer service costs and improving the CX.
- Based in the Czech Republich, Phonexia was founded in 2006 with a vision to provide cutting-edge speech and voice recognition technologies. Phonexia has a close relationship with the Brno University of Technology, with immediate access to the latest scientific innovations around speech technologies. Phonexia serves governments and businesses across 60 countries and specializes in a wide range of verticals, including banking, insurance, public services, telcos, and utilities.

Value Proposition

- Phonexia Voice Verify uses cutting-edge deep neural networks to deliver fast and accurate verification of extremely short speech (3 seconds for verification). Phonexia provides one of the fastest voice verification processes in the market.
- Phonexia offers extremely high voice biometrics acurracy rates in the industry.
- Customers can quickly evaluate and test Phonexia Voice Verify and can obtain a demo instantly, receive a sandbox in one day, and run a proof of concept in a few weeks.
- Phonexia offers language-independent technologies. For example, if someone in a same customer journey speaks in a different language, Phonexia's technologies can still recognize the user and the meaning of the message.

Product Details and Outcomes

- Phonexia Voice Verify offers accurate and fast voice biometric-based speaker identification and can verify call center clients or the remote employees of virtual call centers based on their voice.
- Use cases include call centers for client verification by agents or by smart IVRs, caller verification for a conversational AI platform (e.g., voicebots and virtual assistants), and employee verification at virtual call centers.
- Phonexia offers Phonexia Speech Platform for integrations through REST APIs. This platform provides speech transcription technology that is language dependent and can transcribe the spoken word into text in 17 languages.
- Phonexia has a customer-focused culture, visible in its excellent post-sales services, and offers best-in-class professional services to support solution customization.

Source: Phonexia; Frost & Sullivan

Legal Disclaimer

Frost & Sullivan is not responsible for any incorrect information supplied by companies or users. Quantitative market information is based primarily on interviews and therefore is subject to fluctuation. Frost & Sullivan research services are limited publications containing valuable market information provided to a select group of customers. Customers acknowledge, when ordering or downloading, that Frost & Sullivan research services are for internal use and not for general publication or disclosure to third parties. No part of this research service may be given, lent, resold, or disclosed to noncustomers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without the permission of the publisher.

For information regarding permission, write to:

Frost & Sullivan

3211 Scott Blvd., Suite 203

Santa Clara, CA 95054