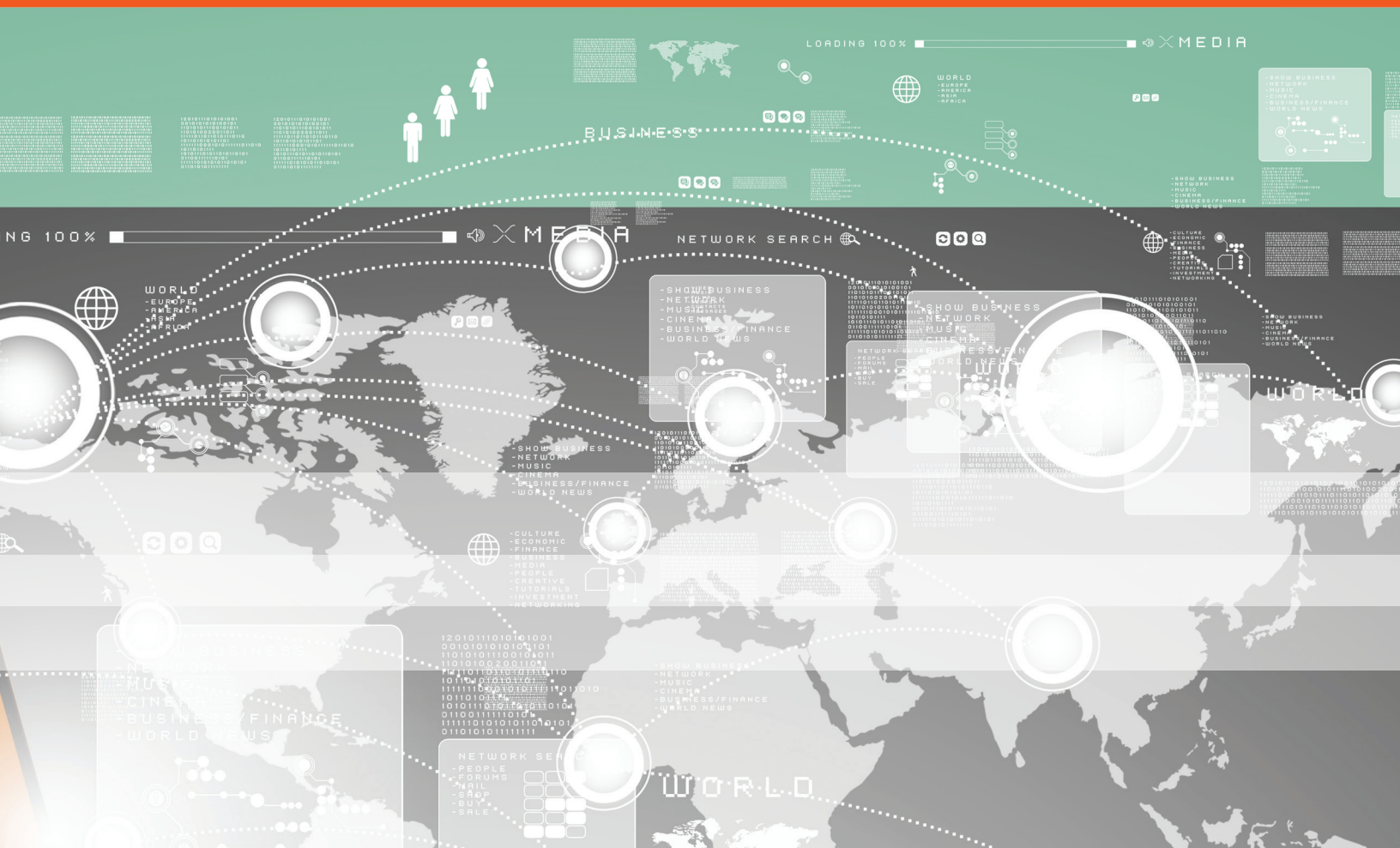
How AI-Based, Zero-Effort Authentication is Changing the Customer Experience

opusresearch



opusresearch | Report »

How AI-Based, Zero-Effort Authentication is Changing the Customer Experience »

New authentication technologies in personalized digital self-service can help in fraud prevention and provide a seamless, almost imperceptible, user experience. "Zero-effort authentication" enables intelligent automation, reduced customer effort (no more PINs and passwords), and improved confidence in security. Enterprises are building zero-effort authentication strategies for greater convenience and less effort to validate a consumer's identity thus increasing customer loyalty and reducing operational costs.

»

January 2019

Ravin Sanjith, Intelligent Authentication, Opus Research

Opus Research, Inc.
893 Hague Ave.
Saint Paul, MN 55104

www.opusresearch.net

The ongoing drumbeat for digital transformation is fundamentally changing how enterprises deliver enriched, personalized customer experiences. With access to mountains of data — scoured, analyzed, and made actionable thanks to Artificial Intelligence, machine learning, and neural networks — enterprise organizations are staking their claim on seamless, context-aware customer interactions as a business differentiator.

With a driving force towards increased digital automation across multiple customer touchpoints, savvy enterprises are creating compelling ways to interact with consumers. The core technologies for a “smart user interface” begin with an enterprise-ready, secure and scalable platform backed up by a set of AI resources, including natural language processing, knowledge management and adaptive authentication. Altogether, these technologies, enhanced through machine learning and neural network processes, help deliver on the promise of secure, personalized digital self-service.

But as customers rely on the ever-growing number of smartphones and connected devices, frequent data breaches are compromising customers' personal data and requiring businesses to implement stricter customer authentication methods. These methods can be time-consuming and highly intrusive resulting in poor user experiences that increase the possibility of customer churn and affect an enterprise's bottom line.

Increasingly, organizations are looking to "zero-effort authentication" that enables intelligent automation, reduced customer effort (no more PINs and passwords), reduced call handling time, and improved confidence in security. These metrics can be optimized for increasing customer loyalty and reducing call center operational costs. Spearheading this era of zero-effort authentication in voice-centric channels are some of the greatest revolutions in speech processing and multi-modal biometrics. For example:

- A new generation of core voice biometric solutions, with advanced AI techniques in speaker recognition is reducing the length of the time it takes to positively authenticate users.
- Together with establishing a correct voiceprint match, enterprises must also adopt liveness detection to protect against additional efforts to through the likes of spoofing with a synthesized voice or a voice recording
- The fusion of voice, face, behavioural, and other biometric modalities are continuously creating opportunities to make seamless, effortless user experiences across a range of channels and interfaces.

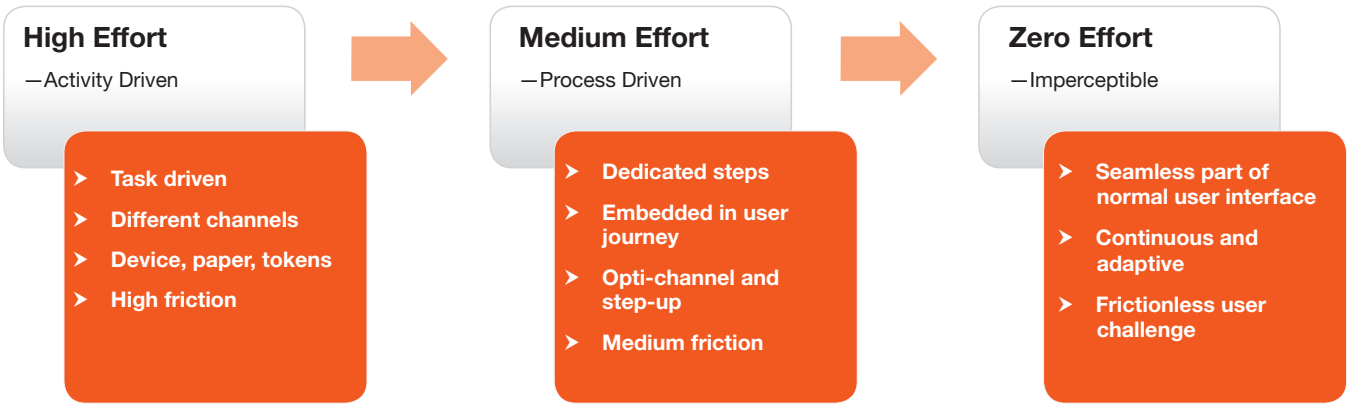
Each of these key areas of technological developments are utilizing new ways to incorporate AI and happening in a time when customers are increasingly locked into their mobile devices.

Comprehensive Security at the Pace of Soaring User Expectations

Smartphones are the bridge between the third industrial revolution (i.e. the Internet), and the fourth (i.e. the Internet of Things, IoT). Where the Internet transformed relationships between firms and their customers, the smartphone has revolutionized all relationships, from normal commerce to deeply personal interactions that transcend generations and cultures. This evolution continues to blur the lines between formal and informal interactions. For example, instant messaging, short text, emojis, selfies and voice-notes are as much a part of

communication among friends, as it is among work colleagues and even customer interactions with their service providers. One of the core drivers of this consistency of behaviour is the smartphone, as the nexus of all these interactions, and the key driver of heightened user experiences.

Users are no longer merely familiar with smartphone and mobile-app capabilities, they demand ease of communication offered across all uses. This, of course, includes enterprise interactions who struggle to combine a simple UX with strong security requirements for payment authentication. Ever since the launch of the first mobile-phone fingerprint sensor on the Motorola Atrox in 2011, self-service authentication has entered the consumer domain. This was in stark contrast with the exclusivity of cross-border, policing and other high-security areas. Over the past two decades, self-service and assisted authentication have progressed from activity based (task driven, high friction), to seamless (low friction, contained within user steps), and now to imperceptible.



From Incremental to Exponential Voice Biometrics Performance

Without delving too deep into the history of biometric authentication, as we are (thankfully) a long way past that, it is important to acknowledge that authentication in general has benefitted from a variety of innovations which have accelerated over time. Biometric authentication is, at the core, a pattern-recognition system which uses probabilistic methods to compute a match/mismatch decision.

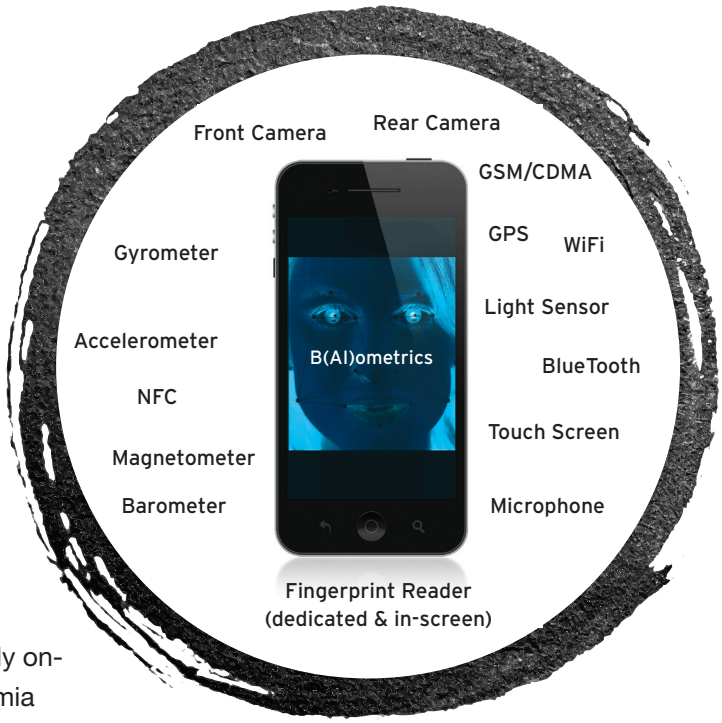
Over time the application of bleeding-edge technologies together with numerous innovative techniques from security and adjacent disciplines has allowed voice biometrics to break through various challenges that presented deployment and adoption challenges.

Requirement	Deployment/Adoption Challenges	Disruptive Innovations
Net Audio Required	Poor UX, Enrolment and Verification	HMM, GMM-MAP, i-Vectors, and now x-Vectors
Audio Formats	High compression codecs requiring up-scaling and transcoding	Availability of cheaper, more cost-effective voice networks
Processing Resources	High cost infrastructures	On-prem, Cloud, On-Device
Cross Channels	Multiple voiceprints and non-interoperability	Neural-Network-based single voiceprint across multiple channel types
Multi-factor	Costs and complexity of integrating different channels and modalities	Single platform Integrated Device, Facial, Behavioural
Spurious Audio	Sneeze, Cough, Dog Bark, Sirens	Acoustic Event Detection
Voice (& text) Chat-based Authentication	Separate processes and too much audio required for reasonable accuracy	Ultra-Short Utterances with less than 1% errors from Advancements in Neural Networking, integrated with meta-data from ML & AI methods
Anti-Spoofing	The use of the same technologies to improve speech technologies is used to spoof systems, e.g. voice synthesis, deep fakes	Neural-Network anti-spoofing with continuous, simultaneous multi-modal authentication

bAIometrics: the virtuous cycle of Biometrics, Sensors, Processing Power and AI

Users are inadvertently adopting sensor usage that includes taking selfies (Google report over 24 billion selfies uploaded in 2017), voice-search via Siri, Google Assistant, Alexa, and of course tapping, texting and swiping in the normal course of smartphone usage.

Consumerization is about simplicity. The interesting contradiction is that it takes high-tech capabilities to deliver this simplicity, and this is made possible by enhanced algorithmic and neural networking methods that are applied to rich sources of data from high quality sensors across facial (high-res front 'selfie' cameras), finger (dedicated and in-screen scanners), location (GPS, WiFi and GSM network), accelerometers and gyrometers . These sensors, combined with the remarkable processing capabilities and storage resources (RAM, embedded and expandable storage) on most mobile devices have are rapidly leading to highly complex, real-time computing that is happening continually on-device. This has shortened the time from academia



to the commercial implementation of AI across smartphones and other 'things' in consumer IoT, such as smart speakers, other connected appliances, homes and automotives which are also increasingly laden with these enabling technologies.

Another exciting development is the use of AI techniques to continually adapt to context, risk, channel and user behaviours in order to optimise the strength and sequence of authentication modality, based the availability of sensor-data at the required time. Cost is also a consideration as there may be material differences in the pricing models, especially from high-end biometrics vendors, and this is also built into the AI models. As the virtuous cycle of biometrics and AI draw them even closer together, we are at the cusp of the next leap forward.

When it comes to authentication, security designers are spoilt for choice in leveraging these capabilities to build highly flexible and accurate systems that deliver seamless experiences that require zero effort and are ultimately imperceptible to the user across web, mobile and all emerging conversational user interfaces.

Ultra-Short Utterance Authentication to Support #VoiceFirst Revolution

Voice continues to grow as a medium of choice across most channels, as well as being the preffered interface in the surging adoption of virtual assistants and smart-speakers. Voice authentication, which meets the required security standards while also delivering conversational UX, has been the challenge in the voice-first domain. This authentication challenge is indeed common across all of IoT and has inhibited the growth of delivering secure personalized services and conduct monetary transactions and payments.

For voice biometrics, the need for lengthy (minimum 3-4 seconds) net user audio has inhibited its use in voice-chat. The ability to combine user utterances starting with device wake up words such as 'Alexa', 'Ok Google' or 'Hey Siri', and combining these ultra-short utterances (sub-1 second) for high quality voice authentication has the potential to unlock immense commercial value. This ranges from requesting high-risk information to authorising transactions to full end-to-end voice shopping.

Enterprises Need Continuously Adaptive Authentication

In addition to short utterance authentication, organizations also need to protect against users changing during the course of interfacing with a system. This may include 'man-in-the-middle' attacks and individuals who initiate a conversation and then 'hot-transfer' to another person. This may be conducted in a 'positive' case, such as a personal assistant call on behalf of a boss, or a son/daughter call on behalf of a parent. But it may equally be a criminal that forces a person to authenticate and then takes over the interaction. It is therefore necessary to continually authenticate the user throughout the interaction while also adapting the biometric modality in use (for example, voice, face, or swipe) to minimize the risk of changing users.

Different biometric methods also consume different resources at differing costs, so it is also necessary to optimize the strength of the authentication based on the available modality as well as the risk associated with the interaction. All of which may also change as the user goes through the journey, shifting channels throughout the interaction, most common switching from 'facetime' to voice-only on an automotive Bluetooth connection.

Why Zero-Effort Authentication is Best Implemented in the Enterprise App

AI methods have come a long way towards supporting adaptive authentication by continuously maintaining channel, device and process awareness. This includes rapidly adapting to changes in a way that is completely seamless to the user and requiring zero-effort. While device manufacturers continue to introduce wider and more sophisticated options for authentication, these present a variety of limitations that necessitate looking beyond a purely manufacturer-led strategy and increase liability concerns. Consequently, the enterprise is best served to implement continuous authentication directly in the enterprise app.

- Most obvious, app updates can be done with greater ease and frequency to adapt to device capabilities, user preferences and evolving attack vectors. Incorporating biometrics in the app by using the raw sensor data allows for a common app across different devices so long as the devices have a microphone and camera plus expose the accelerometer, gyro, and keypress data..

- Relying on the device manufacturer means having to create a different UX for every device. This may be especially challenging transitioning between devices outside of smartphones such as smart speakers, automotive and other connected devices.

- Keeping track of different devices with different capabilities creates highly complex business rules whereas continuous, adaptive authentication built into the app streamlines business logic.

In this age of Conversational Commerce, enterprises are encouraged to seriously consider leveraging the advances in on-device sensor capabilities by overlaying AI-based biometrics ('bAIometrics') within the mobile app to create continuous, adaptive authentication for exponential security at zero-effort customer experience.

About Opus Research

Opus Research is a diversified advisory and analysis firm providing critical insight on software and services that support multimodal customer care. Opus Research is focused on "Conversational Commerce," the merging of intelligent assistant technologies, conversational intelligence, intelligent authentication, enterprise collaboration and digital commerce.

For sales inquires please e-mail info@opusresearch.net or call +1(415) 904-7666