Just showing the finger will do

A leading pink paper recently (Oct 20 2012) reported this "Soon, open a bank account with the swipe of a finger" (http://economictimes.indiatimes.com/news/politics/nation/aadhaar-will-now-be-used-as-identity-proof-for-bank-authentication/articleshow/16884785.cms).

The article states "Submitting photocopies of identity and address proof for opening a bank account, buying insurance or getting a mobile connection could soon be a thing of the past. Instead, it would all be there at your finger tips. The Unique Identification Authority of India (UIDAI) is ready with electronic know-your-customer authentication (eKYC) service which will pave the way to provide identity and address proof by just providing your fingerprints for biometric identification. Officials said the facility of a one-touch eKYC could start as early as next month after government and other agencies, such as Reserve Bank of India (RBI), notify the new norms that explicitly provide for Aadhaar as a valid identity proof".

There are critics and sceptics who assert that the concerned authorities have yet to convincingly talk about, and resolve, critical aspects like data privacy (list of people having access to, say, my biometric data, its links to other data), data security (list of people having access to my data and why they should have access), data integrity (can my data be tampered with? If yes, then remedial measures. What happens if my fingers are temporarily or permanently damaged, disfigured, etc.), and many other aspects.

But for most people, getting the desired service is in itself a distant dream. Take a look at some of the key findings of the first CINDEX of Custommerce released in August 2012, which measured customer experience, their delight and dissatisfaction across categories such as airlines, savings bank, mobile handsets, mobile services, retail, etc.

- Most (98% of a sample 8353) customers cannot recall a great service experience off hand!
- Many brands across categories score low on "treating customers with respect"
- "Delivering on the promise," a high-impact parameter, sees low satisfaction scores among savings bank account holders

As someone said, "A fool with a tool is still a fool." Trouble is, many companies think that merely investing in the latest technology and on-paper systems implies a guarantee of customer service. They could not be more wrong. At the end of the day, it is the person who uses the technology who determines how customers benefit from such technology or

Chandu Nair

A serial entrepreneur who considers himself a marketing professional too. He has marketed and sold products and services both in India and abroad.
chandunair@gmail.com

customers. And that alas, is a place where companies still substantially lag behind.

A study done in January 2012 on banking services in Aligarh district published in the International Journal of Computing and Business Research shows that public sector banks fall much below the perceptions of their customers on all dimensions of service quality. (http://researchmanuscripts.com/IJCBRJanuary2012/7.pdf)

Another study published in Researchers World in 2011 titled "Customer satisfaction in new generation banks (A case study of HDFC Bank)" shows that (to quote verbatim from the study)

- Customers' expectations have gone up manifold
- In the most important categories (Managing accounts and handing enquiries) bank performance is miserable and has totally failed to come true on the expectations of customers
- Regarding the quality of staff, the bank is in a good position
- Over all, out of 31 parameters, bank has failed to satisfy customers in 15 parameters

Today, the marketplace is getting increasingly competitive. Offerings too are increasingly getting to be as pretty similar and are barely differentiated on technical parameters. Service is one thing that can provide a sustained, competitive differentiator. Banking, particularly, is a customer-oriented services industry and continued business depends on ensuring client service and customer satisfaction.

Having the latest technology and spouting the latest buzz words can make you look good for a while. However, it is vital that the general "chaltahai" culture is replaced by a more robust culture of proactive responsiveness.

Voice Biometrics in Authentication

Factors of Authentication

When a person claims a particular identity to gain access to a system to perform an enquiry or transaction, authentication is a process of validating the claim for that identity.

In general, there are three factors to authenticate a person:
First Factor: What you know?
Second Factor: What you have?
Third Factor: What you are?

First Factor (What you know) - Most of the current authentication techniques we use in IVR, Internet, or ATM fall under this factor. It is a means of validating a customer by knowledge on particular information which is presumably known only to them. TPIN, ATM Pin, Password, etc. fall under this category.

Second Factor (What you have) - In this authentication technique the system which authenticates the person tends to validate the person via a unique device which is in position with the person it is trying to authenticate. Unique device, as the name suggest needs to be unique across the globe and cannot be duplicated. RSA SecurID, SafeWord, Vasco etc., which are generally used for authentication for remote login access into an enterprise network fall under this category since these devices are unique and allocated/mapped to a particular person. The one-time password (OTP) mechanism which we use for internet banking and IVR transactions also falls under this category for the simple reason that the mobile number is unique across the globe. When a password is sent via SMS or USSD to that mobile device, then it is assumed the person receiving that information is actually the right customer and they in turn use that information for authentication.

Third Factor (What you are) - In this authentication technique the physical characteristics (face shape, finger prints, voice, etc.) of an individual is used for personal identification. While this is the most accurate method of authentication, this is also the most expensive. There are some practical limitations since some of the biometrics verification techniques require physical presence of a person and specialized interface to accept the inputs. Thus it limits the use of third-factor authentication in many transactions where the person to be validated is not physically present or making the input devices available at remote locations. Voice biometrics is the best choice when it comes to validating a customer/client accessing an enterprise system from a remote location since the investment on specialized interface required to collect the input will not be a challenge. Phones and computer microphones can be used to collect the input and send it to a remote location via PSTN or WAN for validation. Enrolment and verification processes are much simpler in case of voice biometrics and accuracy of voice biometrics is comparable to most of the other biometric techniques used.

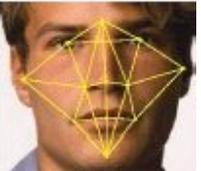## How will Banking/Credit Card Sector Benefit from Voice Biometrics

With the increased patronage of credit and debit card usage, the fraud rate also seems to be climbing which is a concern to banking sector. A leading bank has witnessed maximum 92 frauds of cloning of debit/credit cards or use of fake cards involving over Rs 1.89 crore from 2007-08 to December 2010.

Voice Biometrics helps to address this growing concern efficiently and cost effectively. The introduction of voice biometrics as an additional means of authentication not only ensures the credibility of the authentication mechanism to verify the person using the card, but it also provides a secure feeling against forgery. It encourages customers to use their debit or credit card either in an in-person transaction or online transactions (card-not-present transactions). This moves more cash transactions to the electronic mode to improve banks' profitability.

How it works

Enrollment Process: The customers can be provided a choice either to walk into the nearest branch or reach out to the contact center and get them validated with the contact center representatives. In case they have reached to the contact center the validation can be completely automated via their existing TPIN without any human intervention. In the absence of TPIN the agents validate them through standard set of questions over the phone in case of contact center or by the branch staff in case they are physically present at one of the branch location. Upon the initial validation the callers are connected to the Voice Biometric system which collects the sample from the caller and stores the data in an encrypted format against the customer ID or card number along with their mobile number. If the customer has multiple cards (credit/debit) associated with their customer ID, it is sufficient if to collect the voice sample only once.

Verification Process: Each time a transaction is performed, a request is sent to the Voice Biometric system to verify the authenticity of the customer. This will be in addition to the prevailing validation mechanism, and will be an additional security layer. An outbound call is initiated to the customer, who is requested to authenticate by speaking a pass phrase. Once authenticated, the system sends a notification to the payment gateway or the backend system about the authenticity of the caller.

	Voice	Finger Prints	Retina / Iris	Face Shape
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	High	High
Possible to lose or forget	No	No	No	No

Source: Data monitor

Styles of Verification

One-step: This involves recognition and verification of a unique text in a single step (for example, prompting the customer to speak the debit card number). The advantage of this technique is that the average talk time is reduced and convenient. There is no requirement for a separate password. The flip side is that it is difficult to change the credentials if the access is compromised. This can also confuse the caller into thinking that the access is not secured.

Two-step: In this method a secret password known to the caller is verified. This serves as an additional security since both the voice print and the password content should match. This technique provides the highest security and the flow is well understood by customers. It is also easy to change the password in case the password details are compromised.

Challenge-response: In this method, the system prompts the caller to speak a variable text it plays. The prompt might often be based on repeating random digit strings or a set of pass phrases configured. The advantage of this model is that the customer need not remember any password and resists record and play back attacks and thus useful as a "liveness" test as well.

Application areas

The classic example of biometrics implementation and benefits can be largely felt in the following enterprise areas:

- Password reset applications within a large enterprise where the employees are authenticated using their voice and allowed to reset their passwords.

- Life check for pension fund schemes when the system can call the beneficiaries at regular intervals and authenticate them instead of them producing a medical certificate and be physically present at the fund office for annual life check.

- Second-factor authentication to secure transactions in ATM and merchant transactions.

- In contact centers for fraud/imposter control.

- For remote access control of a computer or physical location where an outbound call can be made to authenticate access control privileges with an administrator and superior before granting permission to the person seeking those privileges.

- As an authentication technique in remote alerting systems for NOC.

- For remote dial-in to manage regular service/back-up activities without being physically present.

Ashok Raj S.
Sr. Technical Architect
Head - Technology and Innovation
CIM Practice
Servion Global Solutions Ltd.
ashok@servion.com

Sansera Engineering Pvt. Ltd.

Sansera Engineering is one of the leading manufacturers and suppliers of precision forged and machined engine components for automobile industries in India and overseas. Sansera was established in 1987 and headquartered at Bangalore. Sansera has its state-of-the-art manufacturing facilities at Bangalore, Manesar (New Delhi), Pune, and Panthnagar. Sansera builds its own CNC-SPMs to be cost-effective and enhance machining capabilities. Sansera has 3000 employees and a turnover of INR 450 Cr (2011-12).

Products:

Sansera offers a comprehensive range of precision forged and machined automobile engine components like rocker arms, connecting rod, crankshaft, gear shifter fork, rocker shaft, intermediate shaft, balance shaft, boss handle, timing sprocket, and arm relay.

Customers:

Domestic: Bajaj Auto Ltd, General Motors India Pvt Ltd, Hero Motors Ltd, Honda Motorcycle & Scooters India Pvt Ltd, Honda Cars India Pvt Ltd, India Yamaha Motors Pvt Ltd, Mahindra Two Wheelers Pvt Ltd, Maruti Suzuki India Ltd, Piaggio Vehicles Pvt Ltd, Royal Enfield, Suzuki Motorcycles India Pvt Ltd, Suzuki Powertrain India, TATA Motors Ltd.

Overseas: Ducati Motor Holding S.p.A .- Italy, Fiat Powertrain - Italy, General Motors - Korea, Harley Davidson Motor Company - USA, MBK Industries - France, Motori Mineralli S.p.A. - Italy, Piaggio - Italy, Polaris Industries - USA, Streparava S.p.A. - Italy, UD Trucks - Japan, Yamaha Motors - Brazil.

Sansera Engineering Pvt. Ltd.
No.261/C, Bommasandra Indl. Area
Bangalore - 560 099, India
Tel: +91 80 27833056, 27833442
Fax: +91 80 27833642
Email: marketing@sanseraindia.com
Website: www.sanseraindia.com