Biometric Identification Evolves to Provide Unprecedented Security & Reliability

Since introduced in 1858 with the first systematic capture of hand images for identification purposes, biometric technology has come a long way. Today, highly advanced, highly accurate biometric technologies can authenticate identity using a person's fingerprint, iris/eye, facial features, and voice, to name a few. With the rise in identity and data theft, the global financial services industry is ramping up its use of biometrics to provide convenient, reliable, and highly secure protection.

FIRST GENERATION

In the 1970s, biometric technology was made available for the first time for:

- Granting physical access within restricted premises
- Recording attendance and verifying employees
- Providing personal identification and verification

DRAWBACKS: The technology was only available through physical devices, and results were time-consuming to generate and lacked accuracy. Additionally, the technology required data storage. Since intranets were at their nascent stages, access to biometric technology was limited and inefficient.

SECOND GENERATION

In the 1990s, popularity of biometrics gave rise to improved technology and faster, more accurate results. The first semi-automated facial recognition system was deployed in 1991, but still required use of an on-site physical device. Computers were used to store data and records without direct involvement in the process.

1992
Biometric Consortium is established within U.S. Government

1994
First iris recognition algorithm is patented

1995
Iris prototype becomes available as a commercial product

1998
FBI launches DNA Index System (CODIS) to digitally store, search, and retrieve DNA markers for forensic purposes

1999
FBI's large-scale ten-fingerprint (open-set) identification system becomes operational, allowing fingerprints to be searched against data on another system

DRAWBACKS: While accuracy improved, the technology was still dependent on a user's physical presence and availability limited to government agencies, FBI, and police departments.

THIRD GENERATION

In the 21st century, use of biometrics expands significantly as the technology improves and availability of mobile phones and laptops goes mainstream. However, mobility for biometrics is only available through handheld and other connected devices. Demand for stronger security pushes a worldwide drive to implement biometrics across a variety of governmental agencies and industries, including financial services, fueling the next wave of technology improvements.

2002
ISO/IEC standards committee on biometrics is established

2003
Formal U.S. Government activities begin; International Civil Aviation Organization (ICAO) adopts blueprint to integrate biometrics into machine readable travel documents

2004
Presidential directive drives government-wide personal identification card for all federal employees and contractors

Bank of Tokyo-Mitsubishi UFJ introduces biometrics at ATMs, using hand and finger scans to authenticate customers

DRAWBACKS: Technology still doesn't achieve 100% accuracy and requires a physical presence. Increased access to technology creates threats from Internet hackers.

CURRENT GENERATION

Smartphone advances and widespread Internet connectivity generate a significant evolution of biometrics as an identity authentication solution enabling the verification of anyone from anywhere.

2010
Poland's cooperative BPS bank installs first biometric ATM in Europe

2011
Motorola introduces first smartphone with fingerprint scanning capabilities

2012
The FIDO (Fast IDentity Online) Alliance is formed to deliver standards for simpler, stronger authentication

2013
Apple introduces Touch ID, a fingerprint recognition feature stored on a user's local device, rather than on Apple services or iCloud

Barclays Wealth becomes first financial services firm to deploy voice biometrics to authenticate customers to their call centers

2016
HSBC and its Internet-based retail bank First Direct announce they will offer 5 million customers access to online and phone accounts using their fingerprint or voice

Banks are testing and adopting biometrics to secure mobile apps.
Many banks already offer fingerprint authentication, and fast movers have also adopted or are testing other modes.

With identity theft, data breaches, and financial fraud on the rise, the financial services industry has turned to biometrics as a security method that far exceeds existing approaches in strength, accuracy, and ease of use. At a time when customers are demanding stronger security to protect their information, yet still want convenience and a great customer experience, biometrics is a smart addition to any company's security strategy.

For more information on biometric authetication solutions for financial services, visit www.samsungsdsa.com/FIDO-biometric-authentication

/SamsungSDSA @SamsungSDSA

SAMSUNG SDS AMERICA SAMSUNG

Sources:
https://securityintelligence.com/momentum-picks-up-for-biometric-security-in-the-financial-sector/
http://authenticid.co/blog/2014/09/30/evolution-of-biometrics-as-an-identity-authentication-technology/
http://celent.com/reports/biometric-atms-japan-fighting-fraud-vein-pattern-authentication
http://www.cnn.com/2010/WORLD/europe/07/05/first.biometric.atm.europe/
https://www.theguardian.com/business/2016/feb/19/hsbc-rolls-out-voice-touch-id-security-bank-customers

Copyright © 2016 Samsung SDS America, Inc. All rights reserved.