You will never need a password again.

Your biological makeup is the key to your individual identity, and soon, it will become the key to safeguarding it.

Each person has a unique biological identity and behind all that is data. Biometric data – facial definitions, retinal scans and voice files – that can be composited through software to build your DNA unique online password or security profile.

Imagine you will be able to walk up to an ATM machine to securely withdraw money by simply speaking your name or looking into the camera. And you can do the same to check your account balance off your smartphone or tablet. You will never need to create, track or remember multiple passwords for various log-ins again.

Mobility is the biggest concern for security and authentication. As devices move from the desktop to your pocket, it becomes easier for a device to get lost or stolen and for your information to fall into the wrong hands. When these things happen, it becomes even more important that a system can quickly verify and authorize that the device is being used by the right person.

IBM scientists have developed technologies that use speech recognition to determine and authenticate user identities based on voice analysis and are now incorporating other biometrics such as face, iris and gesture to leverage for security benefits.

Referred to as multifactor biometrics, smarter systems will be able to aggregate this data in real-time to make sure whenever someone is attempting to access your information, it matches your unique biometric profile and it is authentic. To be trusted, such systems should be able to opt in or out of whatever information you choose to provide.