Biometrics in Intelligent Hardware & Artificial Intelligence | PISIQ

What is Biometrics?

Biometrics in Robotics are physical or behavioral human characteristics to that can be used to digitally identify a person to grant access to systems, devices or data.

Examples of these biometric identifiers are fingerprints, facial patterns, voice or typing cadence. Each of these identifiers is considered unique to the individual, and they may be used in combination to ensure greater accuracy of identification.

Because biometrics can provide a reasonable level of confidence in authenticating a person with less friction for the user, it has the potential to dramatically improve **enterprise security**. **Computers, Robotics**, **Artificial Intelligence (AI)** **and** **Internet of Things (IoT)** devices can unlock automatically when they detect the fingerprints of an approved user. Server room doors can swing open when they recognize the faces of trusted system administrators. Help desk systems might automatically pull up all relevant information when they recognize an employee's

voice on the support line.

According to a recent Ping Identity survey, 92 percent of enterprises rank biometric authentication as an "effective" or "very effective" to secure identity data stored on premises which is connected to Internet of Things (IoT), and 86 percent say it is effective for protecting data stored in a public cloud. Another survey, released last year by Spiceworks, reports that 62 percent of companies such as PISIQ are already using biometric authentication, and another 24 percent plan to deploy it within the next two years.

However, companies need to be careful about how they roll out their biometric authentication robotics systems to avoid infringing on employee or customer privacy or improperly exposing sensitive information that's connected to the Internet of Things (IoT). After all, while it's easy to issue a new password when the old one has been compromised, one simply can't issue someone a new eyeball.

According to the Spiceworks survey, 48 percent cite the risks of stolen biometric data as a top security risk with the technology. Other barriers to adoption include costs, cited by 67 percent of respondents, followed by reliability concerns at 59 percent.

For companies specifically using biometrics to secure IT infrastructure in cloud, Internet of Things (IoT) connected devices, Artificial Intelligence software (AI), Robotics, SaaS, on-prem and hybrid environments, adoption rates are even lower, according to the Ping Identity survey. Only 28 percent of companies use biometrics on premises, and even fewer, 22 percent, use it for cloud applications.