Lumidigm

MATRIX SECURITY SOLUTIONS

Implementing Biometric Technology

Sujan Parthasaradhi
Director of Biometric Applications, APAC, Lumidigm (A part of HID Global)

Biometric Technology continues to gain importance day by day. Two leading brands contribute their inputs to some commonly asked questions

Ganesh Jivani
Managing Director
Matrix Comsec, India

IndiaSAFE: What are the latest trends in biometrics?

Sujan Parthasaradhi: Apple introduced biometrics to millions of people with a fingerprint sensor on some iPhones and Samsung has followed suit. Indeed, the simplicity of the fingerprint biometric on the iPhone has encouraged people who couldn't be bothered with PINs to lock their phones for the first time! The inherent convenience of using biometrics to secure access is the beginning of a trend that will see biometrics appearing on all types of smart devices.

This, in turn, will generate demand for biometrics to be incorporated into a wider range of applications. People are increasingly aware of the importance of keeping their private data and information safe, especially with the increase in online security breaches and identity theft. Users are becoming more accustomed to the use of fingerprint biometrics and they will demand the same level of security and convenience for other times when they need to verify their identity.

Ganesh Jivani: Innovations in biometric technologies are improving reliability and speed of identification. New technologies like palm-vein readers, finger-vein readers and face recognition are widely used and are rapidly improving. Devices today offer better speed, bigger memory and improved aesthetics and ease-of-use.

Access control and time-attendance hardware are evolving from age-old bulk centralized panels to distributed architecture using IP-based intelligent controllers. Software applications are web-based and support mobile applications. IP, Wireless, Mobility and Cloud are the technology trends driving innovation. More and more solutions are moving to IP and offer wireless connectivity. As bandwidth bottlenecks are being removed, enterprise applications are moving to the Cloud, eliminating customer-premise hardware, servers and software.

IndiaSAFE: How has the privacy factor been addressed and what more could be done for the satisfaction of the users?

Sujan Parthasaradhi: Biometric information is not inherently private. We leave our fingerprints everywhere, and hundreds of people see our faces every day. What is private is information that may be accessed by our biometrics, such as name and address, government ID numbers, or our banking activities. Our job in the biometrics industry is to make certain that an unauthorized party cannot access our private data with our biometric information. At Lumidigm, we do that with liveness detection that is field-updatable as new threats emerge.

We also offer hardware and software protection in our tamper-resistant and encryption products. Our customers maintain the privacy of their end-users by deploying secure technologies and by implementing policies that protect biometric and other data.

Ganesh Jivani: On one side security requires mapping people's physical aspects and tracking their movements and whereabouts. On the other side, when we do this, essentially we are trespassing on their privacy. It is always challenging to balance these two seemingly contrasting dimensions. However, it is easier to address privacy when the scope and boundaries are properly defined and understood by everyone involved.

IndiaSAFE: What are the roles of the technology in the present scenario of security and safety?

Sujan Parthasaradhi: The best use of technology is to enhance security without creating barriers for legitimate users. Too often a technology prevents unauthorized access but also makes it really hard for legitimate users to use. The last thing a welfare scheme should do, for example, is prevent fraud at the expense of an intended recipient who cannot prove his identity simply because his card was stolen or the sensor cannot read his worn fingerprint. Biometric technology is available today that is reliable, secure and convenient.

Ganesh Jivani: We live in an era where all aspects of our life are technology-enabled and technology-driven. It is impossible to even imagine any sphere of life without technology. Security and safety are the most fundamental motivators and therefore of prime importance. No wonder, technology plays a vital role in security and safety, and improving in synchronization with improvements in technology. In fact, security and safety attract the largest number of applications for cutting-edge technological innovations.

Technology was invented to improve human safety and security. With proliferation of technology, man started worrying about securing the very same technology created in the first place to protect humans. And thus this virtuous circle of technology-securing-man and man- securing-technology continues improving quality of life.

IndiaSAFE: What are the hurdles/ limitations that you observe in the making and implementation of biometric solutions, especially in India?

Sujan Parthasaradhi: The fingerprint biometric programs in India are facing the major challenge of obtaining good quality fingerprint images and biometric data with the representative population in the field.

Our fingerprint biometric technology, called multispectral imaging, has been deployed around the world for several years now. Multispectral imaging technology collects fingerprint data from both the surface and subsurface of the skin. When the fingerprint ridges at the surface are difficult to distinguish due to age, dirt finger placement, or even normal environmental conditions (dry or humid climate), multispectral imaging technology is able to collect enough relevant subsurface fingerprint data to return a high-quality image. This capability means multispectral sensors provide highly accurate biometric data even in adverse conditions where conventional fingerprint technologies fail. It also means that multispectral imaging is able to provide superior fake fingerprint (spoof) detection.

However, in India, certifications are given more importance than the high biometric performance in the real world field conditions. Most of the certification processes includes testing in a controlled environment which is significantly different to the target environment (with the representative population). In addition, the testing does not take into consideration the fake finger detection capabilities of fingerprint technologies, which is critical for ID management projects in banking, defense and border control areas.

Ganesh Jivani: The first and foremost is biometric technologies are not 100% matured. There are a few constraints related to identification, speed and ease of use. It is a technological challenge to cover all people of an organization with one biometric technology due to wide variation in physical attributes of people including gender, age, disabilities and handicaps.

Our job in the biometrics industry is to make certain that an unauthorized party cannot access our private data with our biometric information. At Lumidigm, we do that with liveness detection that is field-updatable as new threats emerge.

– Sujan Parthasaradhi

Director of Biometric Applications, APAC, Lumidigm (A part of HID Global)

Second, application environments are widely varied. Offices, factories, R&D labs, schools, mines and construction sites – all these applications greatly vary from each other.

Hygiene and ease-of-use are also concerns for many people in many organizations. Many biometric technologies require contact with sensors leading to hygiene fears. Many biometrics such as iris and retina scan technologies require users to position their eyes at specific locations making them difficult and slow.

Next, cost of high-quality biometric devices is still not in the range suitable for commercial deployment.

Last is portability. Most biometric technologies consume comparatively more power making them unwieldy for portable applications.

IndiaSAFE: Which verticals can biometric technology be utilized most efficiently in, and which do you find the best to work in?

Sujan Parthasaradhi: Biometrics work well any time it's necessary to know who is transacting. The government sector has always led here, but the banking and healthcare industries are adopting biometric solutions that protect sensitive data from hackers and other unauthorized users. Sometimes a biometrics solution is the most convenient authentication option. If the biometric sensor chosen is a high-performing one, it can be quicker and easier to place a finger on a sensor than to fumble for a card or remember a password. And of course, biometrics should always be a component of any high-security application where multi-factor authentication is required.

Ganesh Jivani: At present, fingerprint technology is best suited for normal offices and factory applications with normal security concerns. Palm-vein readers are suitable for high-security, and harsh factory and such other industrial applications.

With proliferation of technology, man started worrying about securing the very same technology created in the first place to protect humans. And thus this virtuous circle of technology-securing-man and man- securing-technology continues improving quality of life.

– Ganesh Jivani

Managing Director, Matrix Comsec, India

IndiaSAFE: What are the products that you have currently launched and those that are in the pipeline?

Sujan Parthasaradhi: Lumidigm's V-Series fingerprint sensors prevent unauthorized access with world-class liveness detection and provide the most reliable means to conveniently authenticate an individual. M-Series fingerprint sensors are smaller than the V-Series, yet still offer best-in-class performance under real world conditions.

Lumidigm was acquired this year by HID Global, a trusted source for secure identity solutions. Look for products from Lumidigm that leverage our multispectral imaging capabilities for biometric and credential authentication on a single, integrated device.

Ganesh Jivani: Matrix has recently launched COSEC VEGA – a new-generation rich door controller series specially designed for access control and time-attendance applications. It supports optical fingerprint reader, proximity/ smart cards/ NFC card reader with 3.5" touch-sense color LCD. It meets IP65 for outdoor applications and supports Ethernet with PoE, Wi-Fi and 3G/ 4G/ LTE connectivity options. COSEC VEGA can store up to 500,000 events.

Matrix has also launched COSEC PATH series door controllers specifically designed for access control applications. These compact, robust and cost-effective controllers blend in any modern building design and assure reliable and long-term performance as sentries at the building gates and doors.

IndiaSAFE: Kindly let us know the 2 major projects that you have taken up in India during this year.

Sujan Parthasaradhi: We are involved in few projects including citizen ID management, access control to critical infrastructure facilities and healthcare management. Due to the agreement with our customers, we cannot share the specific details.

Ganesh Jivani: We have implemented many large projects mainly in enterprise space including Adani Enterprise, L&T, Tata Steel, Reliance Industries, Tyco, BHEL, Sterling & Wilson, Shriram Finance, SBI, RBI, Linde, Tata Steel, Power Grid, Andhra Pradesh Police, Indian Air Force, TCI, Gold's Gym, Apollo Health and Lifestyle and many others. We have also implemented many large projects in South Africa, UAE and Saudi Arabia. ■