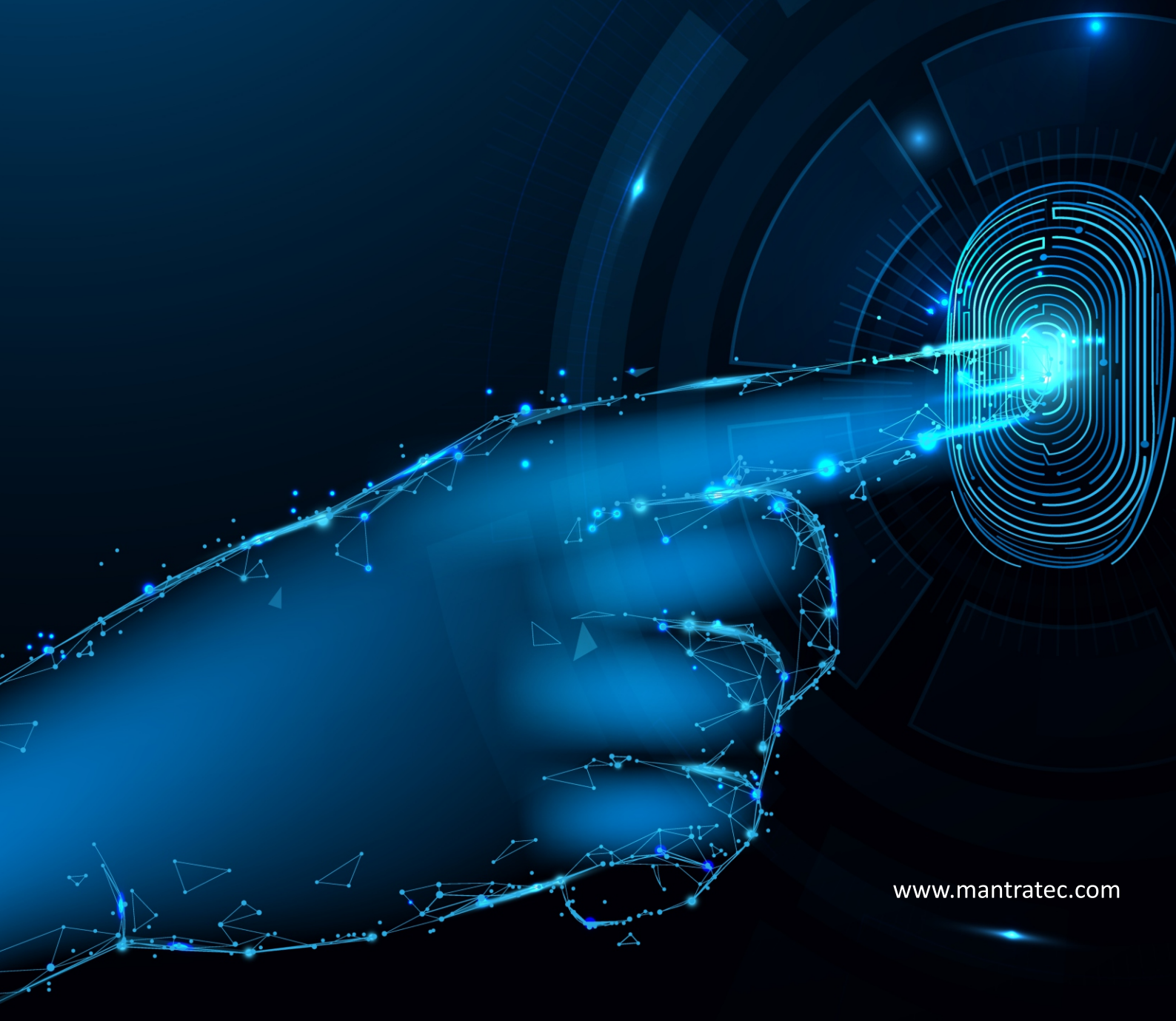
MANTRA

Innovation that counts

Crypto-Biometric Technology

Secure Data with Next-Generation Devices



www.mantratec.com

Table of Contents:

Overview

Biometrics technology is gaining demand across the globe as it is an effective way to identify, recognize and authenticate people through biometric traits like fingerprints, IRIS, Facial recognition and Palm vein. It has gone through many transformations to emerge as the most accurate security option for identification and recognization. Even after technological advancements, there is still room for improvement in the currently used biometric devices. Traditional biometric devices' security limitations led to developing a cryptography-based biometric system, adding an extra layer of data security.

In this document, we will look at the evolution of biometric owing to various security threats. Moreover, we will discuss how cryptography-based biometric devices ensure security to the data and prevent it from threats like spoofing and hacking. This paper also highlights various use cases for this next-generation technology in different industries.

Current Biometric Technology in the Market

The demand for biometric systems is increasing significantly across the world. It is expected that the global market of biometric to cross 68.6 USD billion by 2025 as per the "Markets and Markets" report. The current system uses `physiological and behavioural characteristics, including fingerprints, iris, face, palm, voice, and hand geometry. It has supplanted the security system that relies on PINs, passwords, and smartcards because it is more convenient, fast, and secure. Additionally, it is simple to install and requires no special skills to operate. Both private and public organizations use biometric devices to identify individuals and for managing & monitoring facilities access. Currently, devices are being used widely in all sectors to strengthen access control system for protecting their valuable assets and resources. Apart from this, biometric devices are also employed to make the authentication process safe and seamless for ID management in all sectors.

Limitations of the Current Biometric Devices

There is no denying that traditional biometric devices are used in various industries, but the latest security threats hinder their dependability. Existing devices are vulnerable to multiple security threats like spoofing, tampering, trojan horse attacks, and masquerade attacks. Hackers could steal users' biometric data as well as other personal information. The low effectiveness of current biometric devices to keep data safe and secure gave rise to Crypto-Biometric technology. This next-generation technology adds an extra layer of security to data and protects it from hacking.

Crypto-Biometric Technology Making Mark in the Security Market

Crypto-Biometric Technology can tackle tampering, hacking and other such security threats. The application of cryptographic techniques to biometric features has emerged as a solution to all the threats faced by traditional biometrics. The database encrypted with cryptography makes the devices more secure from threats as a hacker would first need to get access to the encryption keys to steal the data. The promise of the additional layer of security to the data is fueling the demand for Crypto-Biometric Technology in the security market.

Cryptography is mainly used in security systems to protect information. It is possible to access the information by unauthorized persons for different purpose during data transmission over networks. So, it needs to apply preventive and or corrective actions for the enterprise computer network from the intruders for improving security. Cryptography is seen as an effective solution for maintaining secrecy during communication, and cryptographic keys play a vital part in ensuring security.

How Biometric Devices Integrated With Cryptography Works

This framework secures communication between two users using a fingerprint-based crypto-biometric system. First, the feature bit-string is calculated from the users' fingerprint. Next, revocable alteration is applied to derive the private keys of respective users. Then the algorithm is employed to generate public keys from private keys of both sender and receiver, which are shared and further used to create a symmetric cryptographic key at both ends. Here, the biometric data is neither stored nor shared, which ensures data security. Also, precise impertinent secrecy is achieved using session keys.

Advantages of The Cryptography-Based Biometric Devices

The biometric devices encrypted with cryptography come with benefits that help an organization to enhance productivity and efficiency along with keeping the data safe and secure. The advantage of this new next-gen technology are:

- Allows use of a single biometric for many purposes
- It makes the authentication process more secure
- No retention of the biometric template
- High public confidence and acceptance

Mantra Leading the Change with Highly Secure Devices

Mantra is known for its cutting-edge offerings that eliminate verification problem in the existing security system. The company's advanced fingerprint scanner MFS500 LX is highly secure as it encrypts the data within the device only. It comes with a highly accurate and scratch-free figure print scanner capable of detecting counterfeit fingerprints.

MFS500LX

Optical Fingerprint Scanner

Use cases

Bank and Financial Services

The highly secure biometric device assists banks and financial institutions in reducing fraud and protecting confidential data. It is a primary concern for banks to protect financial transactions and allow only authorized person to conduct such transaction. The adoption of crypto-based biometrics could aid the sector in providing easy access to bank services while posing no security risk. The new technology allows bank customers to withdraw money using their biometric traits safely and securely, as it protects the customers' biometric templates from being hacked.

Aside from protecting data from hackers, banks must ensure that only authorised employees can conduct the eKYC of the customer. The crypto-based Biometric device safeguards bank authorities' biometric templates and prevents them from being misused by unauthorised individuals.

IT and Networking Business

A wide range of IT companies uses biometrics systems for secure login in their Network or database systems. Securing confidential business credentials from being leaked or hacked is a big challenge for IT businesses. Theft of biometric templates by an unauthorized person could result in dire consequences. Adopting Crypto-Biometric technology could prevent the stealing of authorities' biometric traits and protect business information from leakage.

Border and Airport Security

Biometric technology is a powerful tool for ensuring VIP passenger data confidentiality & safety, and also it provides a secure immigration process at the border & airport for passengers. The issue with traditional biometrics devices is that they are vulnerable to security threats, as a hacker could steal and misuse the biometric data of VIP delegates and government officials. The use of a crypto-integrated biometric device could provide additional security to passengers immigration process by encrypting biometric data by using cryptography and also restricts illegal immigrant entry into the country.

Healthcare

Medical research, also known as clinical research, uses a huge amount of data of molecule research for medicine or vaccine development. The research centre prioritizes the security of research data. If the research data reaches the competitors or any other unauthorized person, it can have disastrous consequences. A cryptography-integrated device could protect the clinical trial data and its statistical analysis by adding a security layer to restrict unauthorized person's access to the system.

Defence

The security of a country's defence system is critical. The defence system deals with highly secured information that has a significant impact on a country's safety. The data and information from the defence sector regarding defence projects must not be leaked because it could create a more substantial threat to the nation's security. The protection of the defence data is a big challenge, and this is where crypto-based biometric devices can play a vital role in protecting confidential biometric data of an authorized person who access the data and also safeguard the information of project that only accessed by high-ranking officials or authorized individuals through two-factor authentication, i.e. biometric and pin-based system access control. The crypto devices are developed with the concept that an authorized person's biometric templates should not be stolen and spoofed by invaders.

MANTRA

www.mantratec.com

+91-79-49068001

sales@mantratec.com