ARMATURA

www.armatura.us

Armatura BioCode

An Entrance Control Solution of a Mega size Theme Park in Malaysia

Keeping Your Privacy Only in Your Pocket

Client

SUNWAY Lagoon MALAYSIA

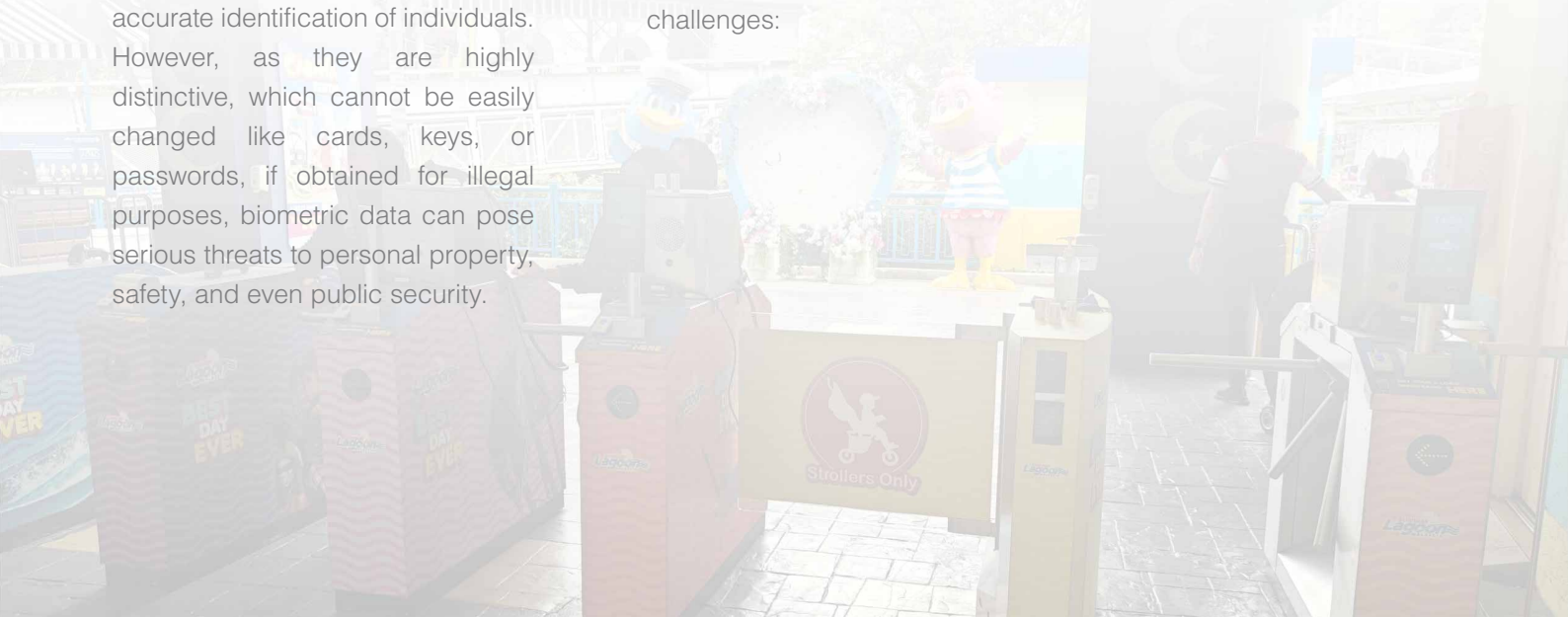
As society's concern for personal privacy continues to grow, people are becoming increasingly concerned about how their personal information is being handled and accessed, especially when it comes to their biometric information, such as faces and fingerprints. Biometric features are unique physical characteristics that can be used for accurate identification of individuals. However, as they are highly distinctive, which cannot be easily changed like cards, keys, or passwords, if obtained for illegal purposes, biometric data can pose serious threats to personal property, safety, and even public security.

Requirement

More Efficient Identity Recognition

Armatura's client for this solution is a large theme park located in Malaysia, and they demanded a more efficient entrance management solution, as the theme park sees thousands of visitors entering daily, and during peak seasons the numbers can reach tens of thousands. Visitors enter the park using purchased tickets. However, many individuals tend to reuse the same ticket for multiple entries. If manual verification of each visitor's identity is required, it would not only consume a significant amount of manpower, but also severely impact the entrance time, affecting the overall visitor experience.

To achieve effective identity authentication, biometric identification is considered an optimal choice. However, applying conventional biometric identification in a setting like a theme park can pose several challenges:



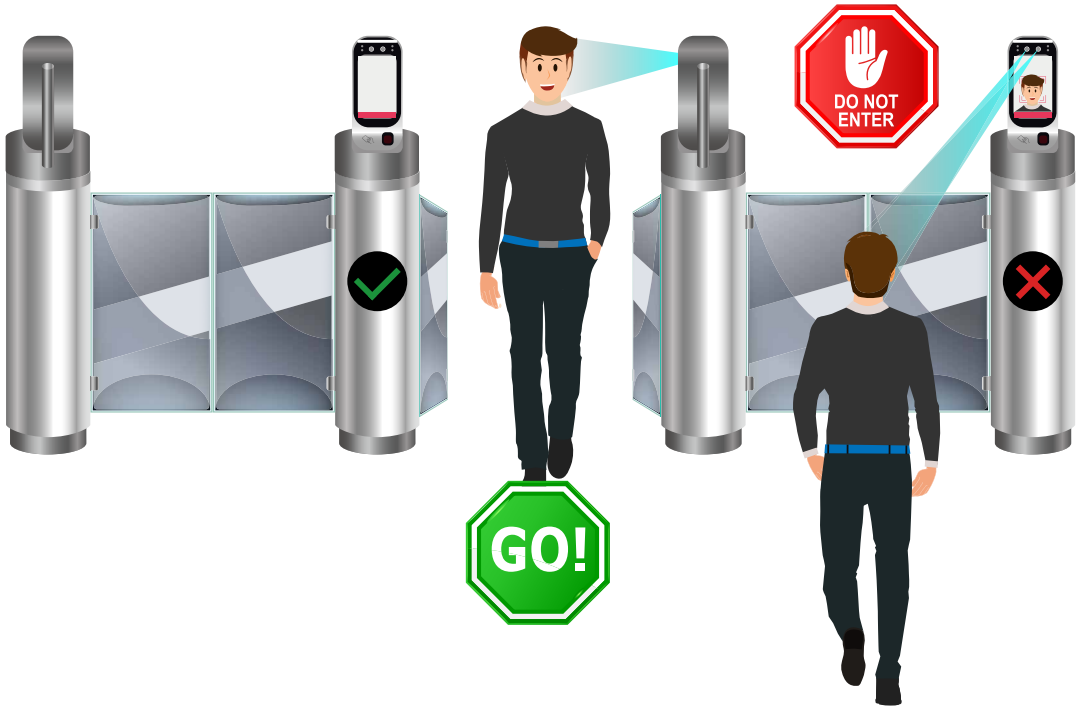
Limitations of Storing Biometric Data

Risk of Biometric Data Storage

Identification systems often require the establishment of large biometric template database, which may include sensitive information such as facial images and fingerprint data. If these data are obtained or misused by unauthorized individuals, it can have a severe impact on personal privacy.

Biometric systems typically collect users' biometric features and store them in a database for identity verification purposes, is known as 1:N verification, where a user's biometric data is compared against multiple biometric templates in the database to find a match, resulting in successful identification. However, biometric data itself is sensitive personal information, and if the database is accessed by unauthorized individuals and used for unlawful purposes, it can significantly compromise personal privacy.

As the client is a large theme park that receives a substantial number of local and foreign visitors, any privacy breach can have severe consequences and potentially lead to significant legal ramifications.



High Standards of Configuration Required

Another major limitation of storing biometric data is the demand it places on system configuration. Large-scale biometric systems require storing a vast amount of users' biometric t for matching purposes. The need to process a large number of biometric templates within a short period of time imposes extremely high requirements on system configuration and performance, resulting in relatively higher costs for the solution.

With thousands of visitors daily, many of whom are first-time attendees, it is evident that using a 1:N biometric identification approach would lead to an exponential increase in the amount of data stored in the database. It would quickly become overwhelming and unsustainable, and continuously upgrading the system configuration is of no feasibility.

Low Verification Speed

Due to the need to compare a user's biometric features with a large number of biometric templates in the database for 1:N identification, it requires much more time. As a result, 1:N biometric identification typically requires more time and computational resources, which can be problematic for applications that require efficient identification, especially when dealing with a large number of users.

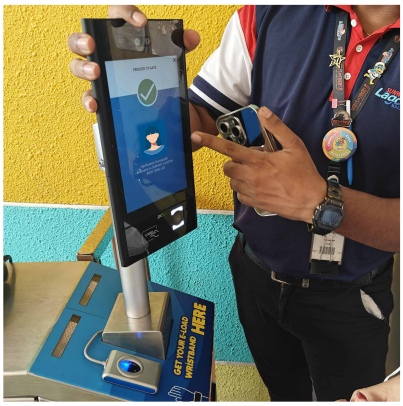
Not Using Biometric Recognition is a Solution?

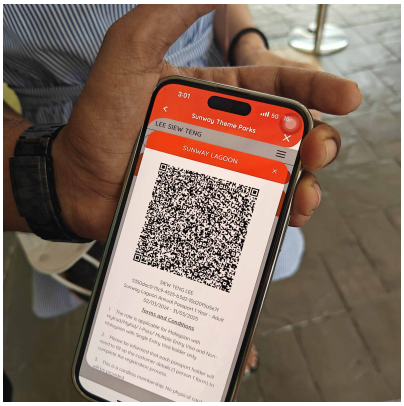
Abandoning biometric identification may prevent the storage of biometric features in databases, but using traditional identification methods such as keys, cards, or passwords cannot guarantee accurate identification, resulting in even greater security risks.

In addition, non-biometric methods, including physical cards and keys, or passwords, are not necessarily more difficult to steal or lose compared to biometric data. Therefore, they only provide temporary solutions rather than addressing the root issue.

To achieve security, the key lies in effectively safeguarding personal privacy and preventing data breaches while maintaining efficient operations when using biometric identification. The development of Armatura BioCode aims to address these challenges in biometric identification.

Armatura BioCode SDK Solution





Armatura integrated BioCode SDK (Software Development Kit) into the Theme Park's ticketing system, and installed ZKTeco's G5 Multi-biometric authentication access control terminals to enable biometric authentication.

Ticket Purchase

When purchasing tickets, customers are enabled to use the Theme Park's mobile app to purchase their tickets via mobile devices with embedded cameras, and the cameras are used for capturing biometric features. A customer is only required to have face or palm scanned by the camera of the mobile device. The BioCode, which is integrated with the app, captures the needed biometrics features for identity verification, then converts the biometric data into a QR code, and is stored in the customer's mobile device.

Entry to the Park

Once registration is successful, the customer obtains a digital ticket with a QR code for access to the Theme Park. Upon arrival to the main entrance of the Park, the customer is required to present his QR code to the G5 Terminals.

ZKTeco G5 is a biometric standalone terminal capable of verifying faces and palms, as well as reading QR codes. G5 Terminals are responsible for reading the QR code stored in the customer's mobile device, and, upon confirmation of the authenticity of the code, scanning the customer's face or palm to obtain biometric features, and comparing the biometric data with the scanned biometric features to authenticate the true identity of the ticket holder.

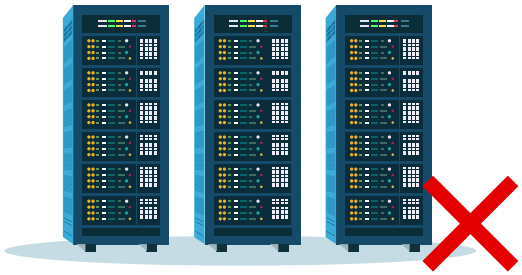
Once the identity is successfully authenticated, the ticket holder will be granted access to the Park, and the entire procedure of authentication is 1:1. Throughout the entire process, the biometric data is only stored on the ticket holder's personal device, and the theme park's system does not establish any database for the storage of biometric data.

Advantages

Security Protection

Biometric Data only Stored Within Users' Devices

BioCode is a solution designed to prioritize the security of users' biometric data and personal privacy. Therefore, when performing biometric feature extraction, all captured biometric data are solely store within the users' own mobile devices, but not stored in any other third-party software or hardware. When authentication, the G5 Terminals only scan users' biometric features, read the biometric data in the users' mobile devices, and compare the two sets of biometric data. Upon completion of authentication, no biometric data is stored in the entire system, and users always have the ability to delete any biometric data in the devices. Users thus have full control over their biometric information.



Prevention Against Biometric Data Theft via Reverse Engineering

As a component of the Armatura suite of solutions, the BioCode employs advanced Armatura biometric algorithms, which enable prevention of reverse engineering to illegally obtain users' biometric data, as it only extracts certain critical biometric features, instead of extracting the entire biometric images or raw data, and the features are well encrypted. Armatura's biometric algorithms are capable of generating identifiable biometric data for precise authentication of identity. The measure effectively protects personal privacy and the safety of users' biometric data, as it does not require complete extraction or storage of entire biometric images. Even if the extract biometric data is obtained, it is impossible to reverse engineer it into a complete biometric image for violation of personal privacy.

AES256 Encryption Protection

To ensure protection of users' personal privacy, AES256 encryption are applied to secure the transmission of biometric data. In the data transmission process, the data is divided into numerous small chunks, and each chunk is encrypted with AES256 standard, the encrypted data is transmitted through a secure channel, and pre-negotiated keys are utilized to ensure that only the intended recipient with the correct key can decrypt the data. AES256 ensures that only authorized recipients can decrypt and access the data, to achieve confidentiality and security of the biometric data.

Efficiency

SDK for Flexible Third-party Integration

BioCode is a versatile biometric solution that can be applied in various application scenarios. To ensure that our solution is accessible to a wide range of users, BioCode is designed as an open-end solution, which means Armatura provides a software development kit (SDK) for third-party development usage, enabling third-party mobile apps and systems to integrate seamlessly with the BioCode solution. Instead of high cost of developing a new system, BioCode enables users to capitalize on their own systems and empower them with biometric authentication function for lowered cost but enhanced efficiency.

Quick and Large-scale Identity Authentication

Due to the entire identification process of BioCode being performed exclusively on the front-end devices, including encryption, QR code generation and decryption, all user data is stored only on their personal devices. The biometric terminal only reads the QR code data from their devices. In addition to ensuring privacy and security, another significant advantage is the elimination of the time required to extract data from a large database. The time for comparing the user's face or palm biometric templates with the biometric templates stored in their QR code is greatly reduced, resulting in faster identification speed. It also eliminates the high-specification system configuration costs required for 1:N identification, making it more suitable for scenarios with a large number of users, such as large-scale parks and concerts.

Armatura BioCode offers high scalability and is designed for large-scale biometric identification. It does not require expensive hardware, complex network systems, or numerous servers. It can easily handle biometric identification for millions of users. It is particularly suitable for scenarios that require processing of extremely large-scale biometric data. It provides small, medium, and large organizations with a flexible, cost-effective, and high-performance biometric security solution.

ARMATURA
Address:190 Bluegrass Valley Parkway, Alpharetta, GA 30005
Phone: + 1 (470) 816-1970
Email: sales@armatura.us
Website: www.armatura.us