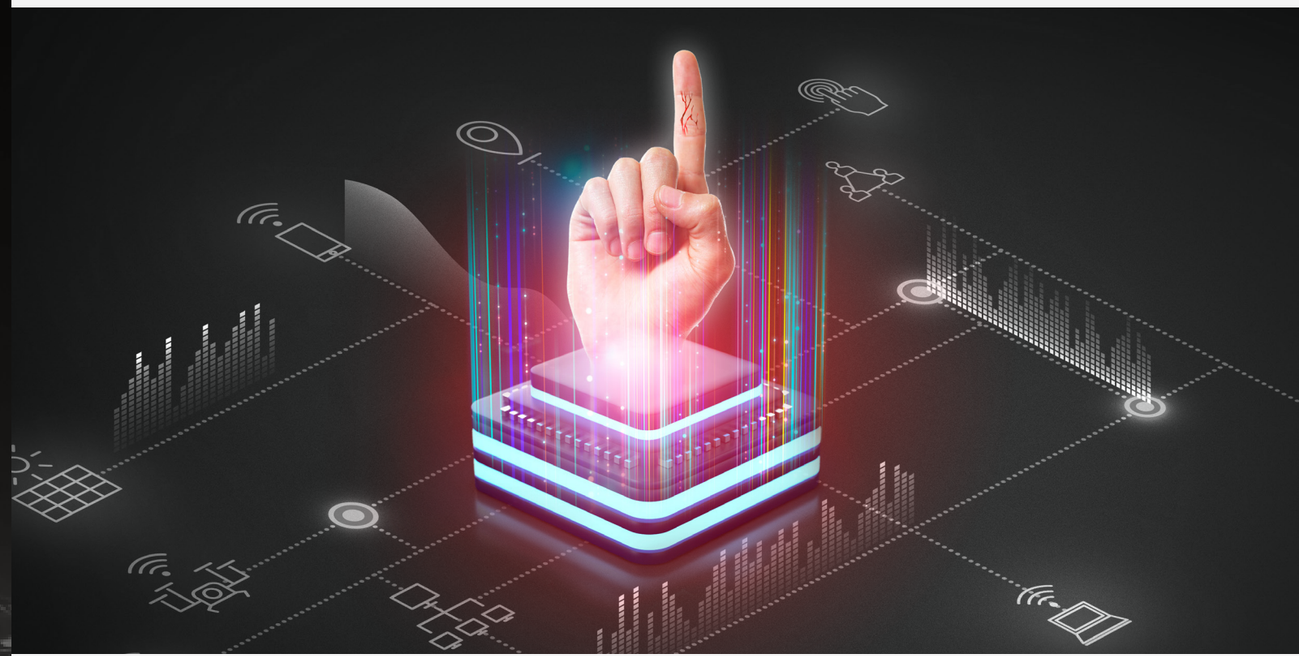

TUNNEL
Tunnel of Biometric
Security Technology

Introduction to Finger Vein Technology

Finger Vein Recognition Technology



Finger Vein Recognition Technology

Finger vein recognition technology is a biometric authentication method that identifies individuals using the unique vein patterns inside their fingers. This technology provides high security and accuracy, as finger vein patterns are inherently unique to each person and cannot be easily replicated externally, making it a highly secure authentication method.

Operating Principle

- **Near-Infrared (IR) Light Transmission**
  - A near-infrared (IR) light source illuminates the finger.
  - Hemoglobin in the blood absorbs near-infrared light, allowing the detection of finger vein positions.
  - The internal finger vein pattern is analyzed by distinguishing areas that absorb light (darker regions) from areas where light passes through (brighter regions).
- **Finger vein Pattern Image Generation**
  - Specialized sensors capture and convert finger vein patterns into images.
  - The captured images are transformed into unique biometric data and securely stored in an encrypted format.
- **Data Comparison and Authentication**
  - During authentication, the newly captured finger vein pattern is compared against the pre-registered pattern data to determine a match.

Features of Finger Vein Recognition Technology

Uniqueness

- Finger vein patterns are unique to each individual, even among identical twins.
  This ensures a high level of security.

Fast Authentication Speed

- The authentication process is completed within one second, enabling real-time authentication.

Anti-Spoofing Protection

- Finger vein patterns are based on subcutaneous blood vessel structures, making them difficult to replicate or forge externally.
- This results in lower susceptibility to spoofing compared to fingerprint or facial recognition.

Biological Response Verification

- The system verifies whether blood is actively flowing (detecting blood circulation) to prevent authentication attempts using artificial models or deceased individuals.

Resistance to External Environmental Factors

- Since veins are located beneath the skin, they are minimally affected by external environmental conditions such as humidity, temperature, and dust, as well as surface conditions of the hand, including cuts, sweat, or oil.

High Durability of Authentication Area

- Since veins are not affected by external damage (e.g., fingerprint wear or facial wrinkles), long-term authentication accuracy is maintained.
- The system is also resistant to issues caused by sweat or oil.

High Accuracy

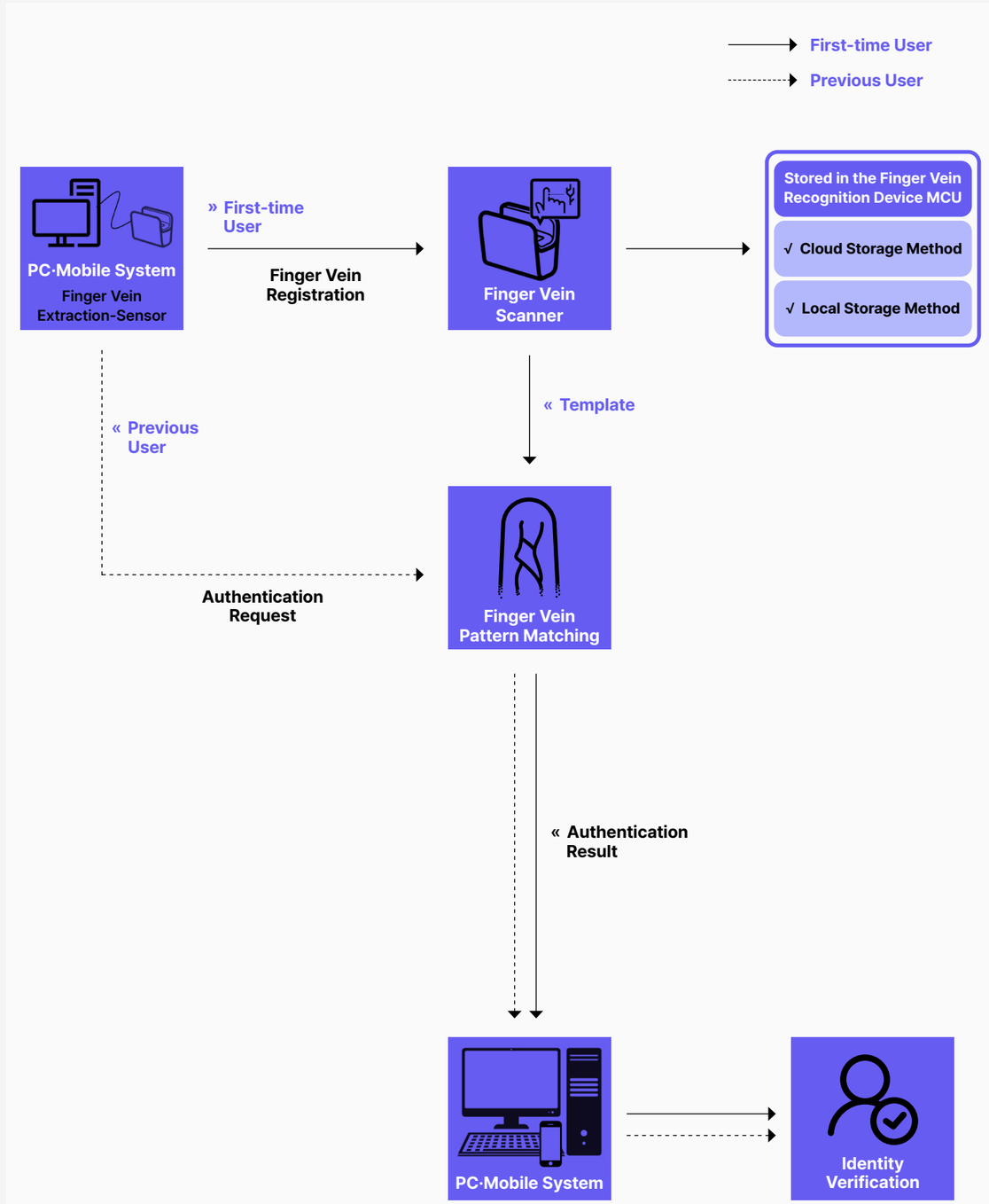
- The authentication process is fast, with low false rejection rates (FRR) and false acceptance rates (FAR), ensuring high reliability.

Multi-Factor Authentication (MFA)

- Finger vein authentication can be integrated with other security measures such as passwords and RFID to enhance overall security levels.

Finger Vein Authentication Process

· The process of extracting Finger vein patterns and verifying them against stored Finger vein patterns for authentication.



Hardware Products

ETUNNEL-ST-100V(Base:Basic Module)

Manufacturer

- ETUNNEL Inc.

Product Overview

- Finger vein authentication device module
- Embedded product for authentication devices

Product Specifications and Key Features			
C-MOS Sensor	· PAG7820LT (SD, Gray Scale, 3.0×3.0μm, Global Shutter)	**LENS**	· FOV : D(88.4°) · TTL: 2.8mm · F-NO. : 2.1
Main Chip	· ARM Cotex-H7	**Interface**	· Bluetooth / HID Connection
Operating System	· Embedded system (Free RTOS, Bare Metal) · Recommended: Windows 10/11 Connection	**Authentication Speed**	· Less than 1 second (Based on Local Max 2 Fingers, 5 users)
Operating Temperature / Humidity	· -20°C~85°C / · up to 90%	**Authentication Method**	· 1:1 Local (Stand-alone) / Up to 1,000 users registered
Product Dimensions	· 33(W)*65(L)*52(H)mm	**Product Weight**	· 45g

ETUNNEL-PL-101V (PC Logon)

Manufacturer

- ETUNNEL Inc.

Product Overview

- Finger vein PC logon recognition device.
- User authentication via finger vein recognition for PC logon.
- Finger vein authentication for enhanced internal access control.
- SSO (Single Sign-On) authentication for medical network access.

Product Specifications and Key Features			
C-MOS Sensor	· PAG7820LT (SD, Gray Scale, 3.0×3.0μm, Global Shutter)	**LENS**	· FOV : D(88.4°) · TTL: 2.8mm · F-NO. : 2.1
Main Chip	· ARM Cotex-H7	**Interface**	· USB 2.0 / HID Connection
Operating System	· Embedded system (Free RTOS, Bare Metal) · Recommended : Windows10/11 Connection	**Authentication Speed**	· Less than 1 second (Based on Local Max 2 Fingers, 5 users)
Operating Temperature / Humidity	· -20°C~85°C / · up to 90%	**Authentication Method**	· 1:1 Local (Stand-alone) / Up to 1,000 users registered
Product Dimensions	· 33(W)*65(L)*58(H)mm	**Product Weight**	· 60g (Base Model 45g + Craddle 15g)

ETUNNEL-SW-100V (Software Wallet)

Manufacturer

- ETUNNEL Inc.

Product Overview

- Finger vein authentication device for creating/ accessing/managing mobile software wallets.
- Finger vein biometric authentication through BLE integration with mobile digital wallets.

Product Specifications and Key Features			
C-MOS Sensor	· PAG7820LT (SD, Gray Scale, 3.0×3.0μm, Global Shutter)	**LENS**	· FOV : D(88.4°) · TTL: 2.8mm · F-NO. : 2.1
Main Chip	· ARM Cotex-H7	**Interface**	· Bluetooth Connection
Operating System	· Embedded system (Free RTOS, Bare Metal) · Android / IOS (App) Connection	**Authentication Speed**	· Less than 1 second (Based on Local Max 2 Fingers, 5 users)
Operating Temperature / Humidity	· -20°C~85°C / · up to 90%	**Authentication Method**	· 1:1 Local (Stand-alone) / Up to 1,000 users registered
Product Dimensions	· 33(W)*65(L)*58(H)mm	**Product Weight**	· 70g (Base Model 45g + Wireless Pack 25g)
Battery	· Lithium Battery 550mAh · Full Charging Time : Within 2 hours	**Number of Authentications Available**	· More than 60 times

ETUNNEL-CW-100V (Hardware Wallet)

Manufacturer

- ETUNNEL Inc.

Product Overview

- Finger vein authentication technology-based cryptocurrency wallet.
- Finger vein biometric authentication data is stored in the Hardware wallet.
- LCD display enables monitoring of cryptocurrency transactions.

Product Specifications and Key Features			
C-MOS Sensor	· PAG7820LT (SD, Gray Scale, 3.0×3.0μm, Global Shutter)	**LENS**	· FOV : D(88.4°) · TTL: 2.8mm · F-NO. : 2.1
Main Chip	· ARM Cotex-H7	**Interface**	· Bluetooth / USB Connection
Operating System	· Embedded system (Free RTOS, Bare Metal) · Android / IOS (App) Connection	**Authentication Speed**	· Less than 1 second (Based on Local Max 2 Fingers, 5 users)
Operating Temperature / Humidity	· -20°C~85°C / · up to 90%	**Authentication Method**	· 1:1 Local (Stand-alone)
Product Dimensions	· 67(W)*40(L)*65.3(H)mm	**Product Weight**	· 70g
Battery	· Lithium Battery 550mAh · Full Charging Time : Within 2 hours	**Number of Authentications Available**	· More than 50 times

Software

Finger Vein Recognition Solution S/W Functions

Credential Provider DLL File

- A Windows component that launches the PC Logon program when the lock screen is activated and unlocks the system after authentication.

PC Logon Components

Administrator Program

- Finger Vein Registration
- Finger Vein Modification
- Finger Vein Deletion

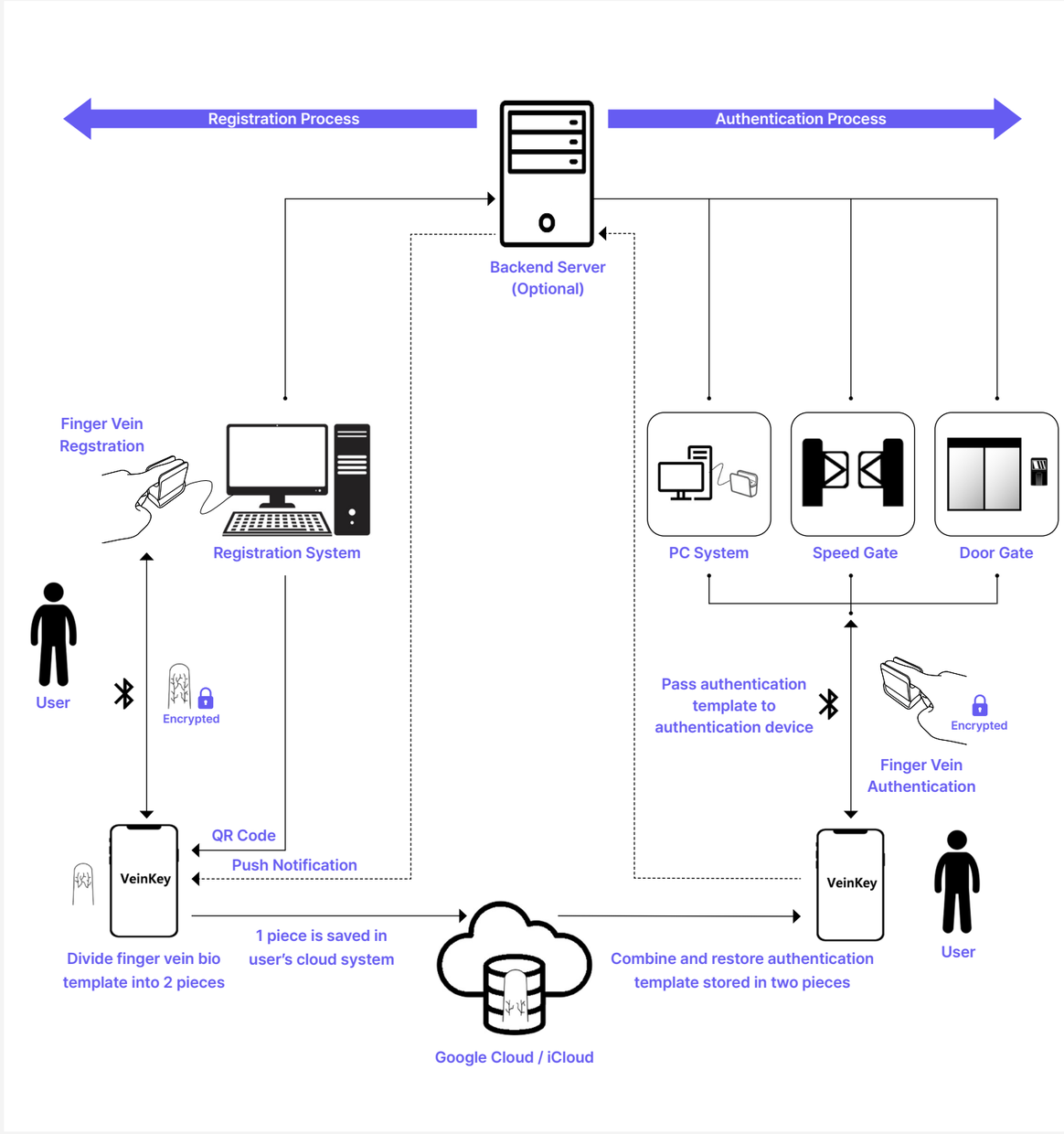
PC Logon Program

- A program executed on the lock screen for finger vein authentication.

Administrator Program (ETL_FVMasterProgram.exe)	
Function	**· Overview: Software responsible for managing finger vein data. Access is restricted to system administrators only.**
Finger Vein Registration	· Registers user finger vein data through the administrator program. · The registered data is encrypted and securely stored.
Finger Vein Modification	· Updates user finger vein data through the administrator program. · Re-registers or updates finger vein data in accordance with security policies.
Finger Vein Deletion	· Deletes user finger vein data through the administrator program. · Deactivates or removes user's account for security reasons.
Credential Provider DLL File	
Function	**· Overview: Provides an interface between the Windows operating system and the PC Logon program. Integrates with the Windows lock screen to process user authentication.**
PC Logon Program Execution (When Lock Screen is Active)	· Integrated with the Windows operating system to perform user logon via finger vein authentication. · Automatically launches the PC Logon program.
User Input Processing	· Collects authentication data through the finger vein system DLL and transfers it to the PC Logon program. · The DLL serves as a data intermediary between the OS and the PC Logon program.
Logon Processing Control	· The DLL transmits the authentication result to Windows. · If authentication fails, the DLL displays an error message and blocks logon access.
PC Logon Program (PCLogon_EXE.exe)	
Function	**· Overview: Delivers finger vein authentication results to the PC.**
Finger Vein Recognition Device Control	· The PC Logon program controls the finger vein recognition device.
Authentication Result Processing	· If authentication is successful, the PC program → CredentialProviderDLL → sends the login signal to Windows.
Security and Log Management	· Logs all authentication attempts and results. · Enables auditing and tracking of security issues in case of problems.

Finger Vein Authentication-Based Identity Verification Platform (VeinKey)

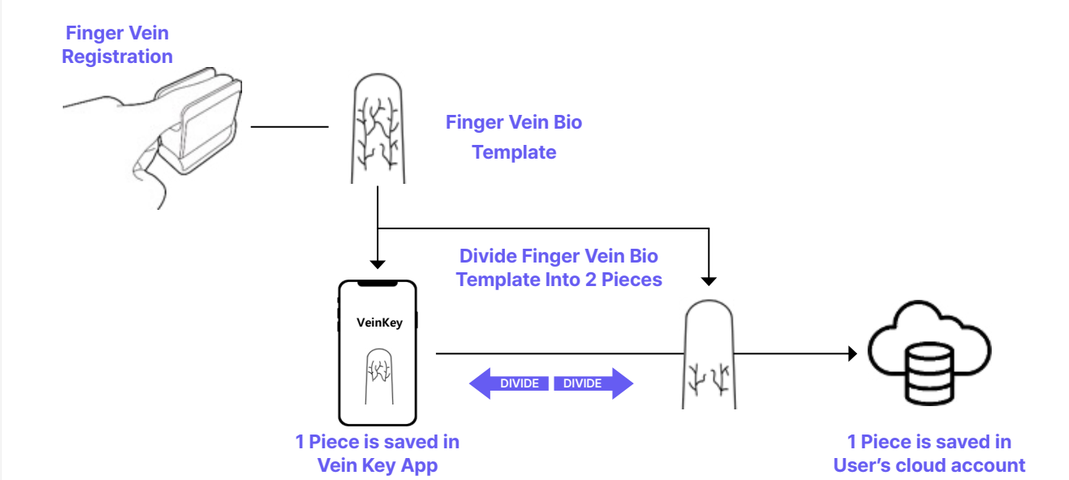
- The **Finger Vein Authentication-Based Identity Verification Platform (VeinKey)** securely registers a user's finger vein authentication data by **splitting and storing** it between the user's smartphone and cloud account during the registration phase. When identity verification is required, the system retrieves the fragmented authentication data from both the smartphone and server, reconstructs it, and uploads it to the authentication terminal for verification. After authentication, the data is immediately deleted. This approach ensures that **users retain full control over their biometric authentication data and perform authentication independently, adhering to the principles of the Self-Sovereign Identity (SSI) platform.**



Core Technology

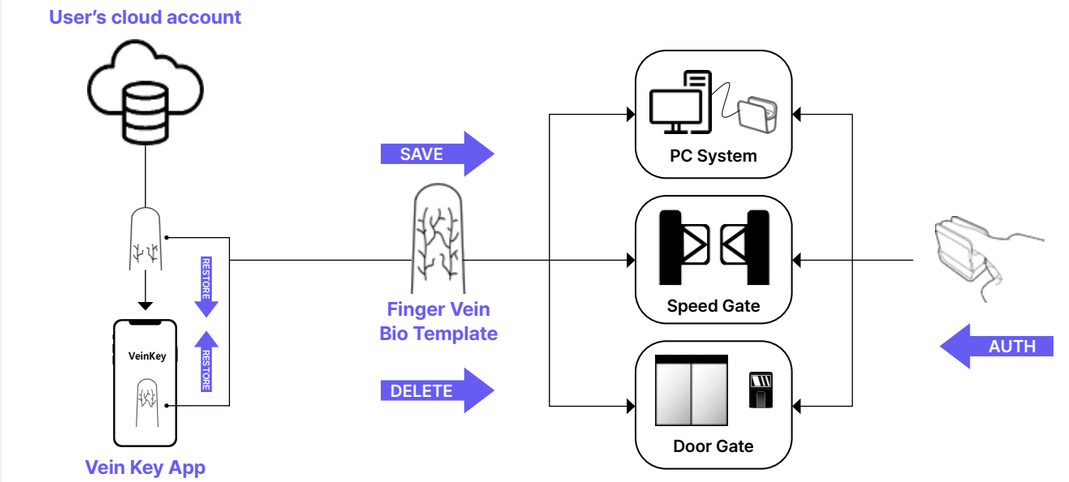
Enhancing Security Through Distributed Storage of Finger vein Authentication Data

- User **finger vein authentication data** is transmitted to a smartphone app and split into two parts: one part is stored locally in the user's smartphone app, while the other is encrypted and securely stored in the user's cloud account. This **distributed storage approach** minimizes the risk of biometric authentication data exposure.



User-Driven Finger vein Authentication via Smartphone

- When authentication is required, the fragmented **finger vein authentication data** is reconstructed on the user's smartphone and then transmitted to the authentication device for verification. Upon successful authentication, the data stored on the authentication device is immediately deleted, ensuring that no sensitive biometric information is exposed or compromised.



Example Use Case (1)

· Visitor Registration and Identity Verification Platform.

Visitor

· 1st Visit I Registration Process

- Visitor Information Check
- Visitor Information Registration
- Additional Visitor Information

- Visitor App Installation Check
- Visitor App Launch (Push/QR Code)

- Automatic Scanner/Device Connection
- Finger Vein Registration
- Finger Vein Authentication (Registration Confirmation)

- Transfer of Finger Vein Authentication Data to a Smartphone
- Deletion of Finger Vein Authentication Data

- Encryption of Finger Vein Authentication Data
- Distributed Storage of Finger Vein Authentication Data

· 2nd Visit I Authentication Process

- Visitor Information Check

- Visitor App Activation (Push/QR Code)

- Automatic Scanner/Device Connection
- Retrieval of Finger Vein Authentication Data
- Transfer of Finger Vein Authentication Data

- Finger Vein Authentication
- Deletion of Finger Vein Authentication Data

- Visitor Identity Verification Complete

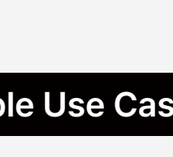
Example Use Case (2)

· Hotel Check-in and Access Management Platform.

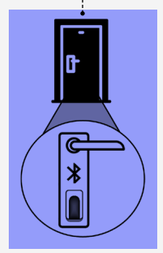
« Reservation Details
« Guest Information
« Guest Bio ID

« Check-in

Guest



« Guest Bio ID
« Access Log



- Reservation Verification
- Guest Information Registration
- Guest App Installation / Activation (Push/QR Code)

- Automatic Scanner/Device Connection
- Finger Vein Registration
- Finger Vein Authentication (Registration Confirmation)

- Transfer of Finger Vein Authentication Data to Smartphone
- Deletion of Finger Vein Authentication Data

- Encryption of Finger Vein Authentication Data
- Distributed Storage of Finger Vein Authentication Data
- Guest Bio ID Creation

- Guest Bio ID QR Code Generation/Scanning/ Storage
- Guest VeinKey Mobile Access Pass Generation

- Move to Assigned Room
- Open VeinKey App (Mobile Access Pass)

- Automatic Door Lock Scan/Connection

- Retrieve Finger Vein Authentication Data
- Transmit Finger Vein Authentication Data

- Authenticate Finger Vein for Door Lock
- Verify Guest Bio ID
- Log Access Entry

- Unlock Door

Application Areas of Finger Vein Authentication Technology

· Finger vein authentication technology is widely used across various industries due to its high security, accuracy, and resistance to forgery.

· Finance & Banking

Used for secure transactions, access control, and identity verification in financial

» ATM Authentication – Replaces PIN-based verification for withdrawals and transactions.
» Mobile Banking & Digital Payments – Enhances security for banking apps and online transactions.
» POS (Point of Sale) Systems – Allows biometric-based payment authorization.
» Branch Access Control – Restricts access to secure banking zones for employees and VIP customers.

· Security & Access Control

Deployed in high-security environments where precise user verification is required.

» Corporate Office Access – Grants entry only to authorized employees.
» Data Centers & Server Rooms – Prevents unauthorized access to critical infrastructure.
» Military & Defense Facilities – Ensures security for restricted government and military areas.
» Research Institutes & Laboratories – Protects sensitive intellectual property and confidential projects.
» Smart Locks & Digital Keycards – Provides biometric authentication for personal or business use.

· Healthcare & Medical Systems

Used to protect patient data, prevent identity fraud, and improve access control.

» Patient Identity Verification – Ensures accurate patient authentication to prevent medical errors.
» Medical Record Access – Restricts access to electronic health records (EHRs) for authorized personnel.
» Secure Drug Dispensing – Prevents prescription fraud and ensures only authorized medical staff can access medications.
» Insurance & Billing Verification – Reduces fraud in medical billing and insurance claims.
» Hospital & Clinic Access – Limits entry to restricted areas such as ICUs and operating rooms.

· Education & Examination Security

Used in academic institutions for attendance tracking, exam security, and campus access.

» School & University Attendance Systems – Ensures accurate attendance records and prevents proxy attendance.
» Exam Candidate Authentication – Verifies student identities before high-stakes exams to prevent impersonation.
» Library & Research Lab Access – Restricts access to registered students and faculty.
» Administrative System Login – Protects student and faculty portals from unauthorized access.

· Government & Public Services

Implemented in e-Government systems, border security, and public safety programs.

» National ID & E-Government Authentication – Used for digital identity verification in various government services.
» Passport & Border Control – Ensures secure traveler identification at immigration checkpoints.
» Voting Systems – Enhances election security by verifying voter identity.
» Welfare & Subsidy Programs – Prevents identity fraud in government benefit distribution.

· Transportation & Logistics

Used to enhance security and efficiency in transportation infrastructure and logistics management.

» Airports & Airline Check-ins – Automates and secures passenger authentication processes.
» Railway & Public Transport Access – Offers biometric-based ticketing and boarding systems.
» Fleet & Cargo Access Control – Secures access to sensitive cargo, transport fleets, and warehouses.
» Ride-Sharing & Car Rental Services – Provides secure driver authentication to prevent vehicle misuse.

· Hospitality & Smart Tourism

Improves guest convenience and security in hotels, resorts, and travel services.

» Hotel Check-in & Room Access – Replaces key cards with biometric room access.
» VIP & Loyalty Programs – Provides seamless and secure authentication for premium services.
» Cruise & Theme Park Entry – Enables fast and fraud-proof access for registered guests.
» Cashless Transactions at Resorts – Allows guests to make purchases without carrying cash or cards.

· Retail & Consumer Applications

Enhances customer security and experience in physical and online shopping.

» Self-checkout & Kiosk Authentication – Speeds up secure payment processes.
» Loyalty Program Memberships – Enables biometric-based loyalty and reward point authentication.
» Restricted Item Sales (Alcohol/Tobacco) – Ensures age verification without requiring ID cards.

· Enterprise IT & Cybersecurity

Strengthens protection against unauthorized access in corporate digital environments.

» PC & System Logins – Enables password-free authentication for secure system access.
» Multi-Factor Authentication (MFA) – Enhances security by combining biometric verification with other authentication factors.
» Cloud & Remote Work Security – Secures access to corporate VPNs and cloud storage.
» Time & Attendance Management – Provides fraud-proof workforce tracking.

Multi Modality

Applications of Finger Vein Technology in Multi-Modal Systems

- **The multimodal method using the P2N2 AI Engine (biometric authentication integrated module)**

- **Enhanced Security**

  Combines multiple biometric authentication methods (e.g., fingerprint, Finger vein, facial recognition) for stronger identity verification.

- **High Accuracy**

  Reduces false positives and negatives by cross-verifying multiple biometric data points.

- **Spoof Prevention**

  Difficult to bypass or fake due to the combination of modalities, ensuring greater reliability.

Contact Us

ETUNNEL Inc.

Address:
Room 1011–1015, Block C, H Business Park, 26,
Beobwon-ro 9-gil, Songpa-gu, 05836 Seoul,
Republic of Korea.

Telephone : +82 2 1899 1959

Fax : +82 2 6281 8777

Business Registration Number: 270-87-02480

Homepage: etunnel.net

E-mail: business@etunnel.net

ETUNNEL