Activation-match: Transforming identity authentication and resource access with independent, multi-modal biometric methods organically interested in superior security and human experience

Introduction

Passwords are outdated and undermine security and user experience. Our problems don't stem from user password selection or poor cyber hygiene; the issue is the unproductive nature of passwords. Users juggle dozens of complex and increasingly uniquely constrained passwords, highlighting the need for a better method of identity authentication and secure resource access. Our vision is simple: maximum security and minimum user effort yields a **trust minimizing framework** for digital and cyber security. We can take a data-centric solution even further by fragmenting and distributing data into incomplete strings across local and cloud data stores and platforms. Doing so leverages independent, distributed systems designed around a **zero-knowledge model** that leaves malicious actors navigating technological confusion. This type of data security model is directly applicable to concepts from in-person healthcare system check-in procedures to privacy-preserving data transport on cloud platforms. We're reimagining identity authentication and human resource access to recognize *users* as humans with physical and digital modals of life.

Solution: Activation-match

The **activation-match method** is an algorithm of next-generation, multi-modal biometric methods we intend to deploy to transform identity authentication and public and private resource access. This method is built on independent biometric processes: for example, with a consumer electronic device, one local process (e.g., fingerprint or palmprint scan) and one cloud-based process (e.g., combination of independent retina, sclera, and iris scans). This design is simultaneous and frictionless for users, mathematically superior to current standards of authentication, and more privacy-preserving than traditional logins or single-biometric methods, given our novel distributed data architecture that further leverages randomization, non-predefined code (e.g., XML), and fragmentation and distribution of data and code strings across encrypted cloud and local data stores.

Key features

- Multi-modal combinations of biometrics: Uses two or more independent biometric processes simultaneously to enhance security and user experience.
- Fragmentation and distribution of data into incomplete data strings.
- Local and cloud-based distributed system: Combines local verification (activator biometric) with cloud-based identification (matcher biometric) methods to ensure robust, resilient security system (through private devices or edge devices).
- Privacy-preserving data architecture: Keeps all personally identifiable information (PII) off the cloud, storing it locally and protecting it through the activation-match process.
    - Code chain randomization and deployment of non-predefined code (e.g., XML).

Applications

Activation-match can replace passwords, passcodes, and PINs. It can support or replace existing standards for secure military installation and secure facility access. It can set a new biometric-based standard of security in digital and in-store payments and financial transactions. It can seamlessly and precisely accomplish many tasks we use QR codes for. It can provide a basis for social media verification badges and can provide actionable protection to dating app users. Activation-match can create more efficient and seamless corporate and residential delivery access, remove the hotel key card (and physical keys), and can integrate into processes that currently use document-based identity authentication. The software development experience and content creation processes and attribution can be transformed with biometric-based credit. We are our own proof of identity and method of authentication, according to activation-match.

Advantages over existing solutions

- **Enhanced security**: Requires spoofing multiple unrelated biometric traits.
- **Eliminates passwords**: Removes phishing targets and user frustration.
- **User-centric workflow**: Guides towards effortless resource access, leveraging the uniqueness of the user as the credential, creating a much wider and granular human biometric profile than that which currently exists, either as a result of siloes or lack of collection.

Security architecture

The activation-match method introduces a novel security architecture that distributes data and trust between the user's device (local data store) or an edge device or other local store and the cloud, while keeping all PII in the local encrypted store. By fragmenting and distributing biometric factors data, we ensure that no single potentially successful malicious action can be actionable or valuable to a malicious actor. Randomized code chain changes and deployment of non-predefined code keep malicious agents on square one.

Device-side security

The fingerprint, palmprint, or other method used as local activator is stored and verified on the user's device or other edge device leveraging a secure local store. Modern smartphones and laptops have secure co-processors or subsystems (like Apple's Secure Enclave) that can store biometric templates and perform matches in an isolated environment. While many companies and solutions deploy this device-side security as an absolute solution currently, we view this solution as having information-bias and thus define it solely as a sufficient verification method (we define authentication as verification and identification, with the latter contributing substantially more resilience to the authentication process).

Server-side security

The retina, sclera, and iris scans are independently and without PII matched against respective global template libraries – a process that combinedly serves as our cloud-based matcher solution. It's a process entirely absent of PII because of indexing to local data stores for private access solutions.

Conclusion

Activation-match offers a seamless, secure, and user-centric solution for identity authentication and resource access. By leveraging multi-modal biometrics and distributed data architecture, we can significantly enhance security that's organically interested in driving better human experience across markets and sectors.