Technical Scientific Report: Systems, Methods, and Devices for Authentication

Abstract (Summary)

This report analyzes a collection of patents related to systems, methods, and devices for authentication. The inventions covered address various challenges in authentication, including improving security, enhancing user convenience, preserving privacy, and adapting to evolving biometric data. The solutions range from multi-factor authentication schemes using biometrics, SMS, and device-bound tokens to privacy-preserving biometric authentication methods employing homomorphic encryption and distributed authentication architectures. These inventions aim to provide more robust and user-friendly authentication mechanisms for a wide range of applications, including e-commerce, banking, physical access control, and device security.

Background and Existing Technologies/Challenges

Conventional authentication methods, such as passwords, are vulnerable to various attacks, including phishing, brute force, and social engineering. Biometric authentication offers a more secure alternative, but it raises concerns about data privacy and the potential for biometric data compromise. Multi-factor authentication (MFA) combines multiple authentication factors to enhance security, but its implementation can be cumbersome and inconvenient for users. Existing systems often rely on trusted third-party servers, which can be a single point of failure and a privacy risk. Furthermore, legacy applications often lack robust authentication mechanisms, and retrofitting them with modern security features can be expensive and error-prone. These patents address these challenges by providing innovative authentication systems, methods, and devices that enhance security, improve user experience, and preserve privacy.

Technical Fields of Invention

The inventions described in the provided patent summaries span several technological areas, including:

- **Biometric Authentication:** Systems and methods for authenticating users based on their unique biological characteristics (EP 3979552, WO 2009153742, WO 2016129453, WO 2017083732, WO 2016099674, WO 2022046181, EP 2199945, WO 2016145454, WO 2016094056, WO

2021085799, WO 2021026464, EP 4050846, EP 4264460, WO 2016145454, EP 2995040, WO 2014182787, WO 2019133339, WO 2016033499, EP 3373554, EP 4050846, EP 4232923).

- **Multi-Factor Authentication (MFA):** Authentication systems that require users to provide multiple authentication factors (WO 2021212351, EP 1841174, WO 2008122108, WO 2023107820, EP 1925113, WO 2016145454, WO 2013159110, WO 2023283499, WO 2023091982, WO 2013019880).
- **Cryptography:** Techniques for secure communication and data protection, including encryption and homomorphic encryption (EP 3979552, WO 2017083732).
- **Network Security:** Methods and systems for protecting computer networks and data from unauthorized access (EP 1841174).
- **Identity Management:** Systems for managing and verifying user identities (WO 2008122108).
- **Mobile Authentication:** Authentication methods specifically designed for mobile devices (WO 2016033499, WO 2021085799).
- **Voice Biometrics:** Authentication systems that use voice recognition technology (WO 2022256595, EP 2560122).
- **Blockchain Technology:** Application of blockchain for secure biometric credit systems (WO 2019133339).
- **Data Processing:** Apparatuses and methods for processing biometric and authentication data (WO 2016099674).
- **Computer User Interfaces:** Design and implementation of user interfaces for biometric authentication systems (EP 4264460).

Inventions Related to Systems, Methods, and Devices for Authentication

Detailed List of Inventions with Novelty and Objectives:

1. **Privacy-Preserving Biometric Authentication (EP 3979552):** This invention introduces a multi-factor biometric authentication method that authenticates a client without relying on a trusted third-party server. It uses Fully Homomorphic Encryption (FHE) to encrypt biometric features on the client-side, allowing the server to perform computations on the encrypted data without decrypting it. This approach preserves the privacy of the biometric data while providing secure authentication. (Relevant)

2. **Enhanced SMS-Based Multifactor Authentication (WO 2021212351):** This invention enhances the security of SMS-based MFA by sending multiple codes to the user and requiring the user to select one or more codes to enter based on instructions from the application and server. This makes it more difficult for attackers to intercept and use the codes. (Relevant)

3. **Multifactor Authentication for Legacy Applications (EP 1841174):** This invention provides a method for adding MFA to legacy applications without rewriting them. It intercepts access attempts, determines if authentication credentials are available based on a policy, and redirects the user to an identity service if credentials are unavailable. (Relevant)

4. **Redundant and Multifactor Authentication with Multiple Identity Providers (WO 2008122108):** This invention eliminates reliance on a single identity provider by using multiple independent IdPs in concert. It requires a combination of credentials to access resources, providing a more secure and reliable identity management system. (Relevant)

5. **Multifactor Authentication System Using Encrypted Authentication Data and Image Enhancement (WO 2023107820):** This invention uses a compressed image of an optical code for authentication. A deep neural network enhances the image to overcome quality issues, and the decoded code is checked for authentication data corresponding to access rights. (Relevant)

6. **Handheld Multi-Factor Authentication Card-Device (EP 1925113):** This invention integrates multiple authentication factors ("what you have," "what you know," "what you are," and "where you are") into a single handheld device. It includes a serial number for "what you have" and a thumbprint sensor for "what you are" authentication. (Relevant)

7. **Sharing Authentication with Shared Session Tokens (WO 2024254315):** This invention reduces duplicative authentications by generating a shared session state that can be reused by different sources requiring authentication. It transmits a first message to an authentication service including shared information and receives a message related to a second authentication to bypass the second authentication. (Relevant)

8. **Biometric Authentication Using Social Network Information (WO 2009153742):** This invention improves biometric authentication by reducing the false acceptance rate. It narrows down the search space during a matching operation using information about a user's social network. (Relevant)

9. **Biometric Authentication Platform System with Originality Control (WO 2016129453):** This invention manages original record correspondence information for biometric information used by multiple services. It uses majority logic to determine authentication results based on biometric information received from these services. (Relevant)

10. **Biometric Data Encryption for Authentication (WO 2017083732):** This invention uses biometric data to encrypt a secret number, forming a biometric public key. This key can be used for enrollment, authentication, establishing a secure communications channel, and cryptographically signing a message. (Relevant)

11. **Distributed Biometric Authentication (WO 2016099674):** This invention distributes the biometric authentication process between an application processor and a secure processor. The application processor performs an initial authentication process, generating authentication parameters that are then used by the secure processor to perform a second authentication process. (Relevant)

12. **Customizable Security Through Biosignal Authentication (WO 2022046181):** This invention enhances security by using authenticated user-administered biometric identification and control systems for authenticating biosignal representations of user-specific gesture-intentions. (Relevant)

13. **Adaptive Biometric Authentication (EP 2199945):** This invention addresses the problem of reduced authentication success rates due to changes in biometric information over time. It uses a first, fast verification process and switches to a second, more precise verification process when the authentication success rate decreases. (Relevant)

14. **User-Selectable Multifactor Authentication (EP 4145312):** This invention improves security and convenience in multifactor

authentication by allowing users to select at least one authentication method. (Relevant)

15. **Proximity-Based Biometric Authentication (WO 2016145454):** This invention requires biometric authentication on an authentication device and proximity between the authentication device and a browsing device. (Relevant)

16. **Combined Biometric Indicator for Multiple Users (WO 2016094056):** This invention receives biometric measurements from multiple users and generates a combined biometric indicator. (Relevant)

17. **Remote Biometric Authentication (WO 2021085799):** This invention involves an electronic device that stores user biometric information and performs authentication in response to requests from other devices, transmitting authentication results without exposing the raw biometric data. (Relevant)

18. **Behavioral Biometric Authentication for Transactions (WO 2021026464):** This invention uses a behavioral biometrics server to assess the authenticity of a transaction based on transaction data and behavioral patterns. (Relevant)

19. **Sharing Biometric Data Across Devices (EP 4050846):** This invention enables the sharing of biometric data across different applications and devices by storing reference biometric data on a backend server. (Relevant)

20. **External Accessory for Biometric Authentication (EP 4264460):** This invention uses an external accessory device to perform a secure operation when biometric data doesn't meet authentication criteria. (Relevant)

21. **Multi-Factor Mobile Transaction Authentication (WO 2013159110):** This invention automatically recognizes, validates, and utilizes different types of information (user, device, network) processed with unique algorithms and encryption as components of a multi-factor authentication process. (Relevant)

22. **High Fidelity Multi-Modal Out-of-Band Biometric Authentication (EP 2995040, WO 2014182787):** This invention uses multiple

biometric inputs received from different input devices on an electronic device. (Relevant)

23. **Biometric Credit Based on Blockchain (WO 2019133339):** This invention provides systems and methods for biometric credit based on blockchain to facilitate payment transactions. (Relevant)

24. **Multi-Channel Authentication (EP 2560122):** This invention employs multiple communication channels and security features, including unique knowledge, unique objects, biometric features, and the ability to respond in a way that a machine cannot imitate. (Relevant)

25. **Secure Cardholder Authentication Using Biometric Data (WO 2016033499):** This invention provides secure multi-factor authentication processes to authenticate a user that utilizes a consumer device, wherein the consumer device is used to capture biometric data from the user and securely compare the captured biometric data to stored biometric templates to authenticate the user. (Relevant)

26. **Multi-Factor Authentication in Virtualized Desktop Environments (WO 2023283499):** This invention addresses the technical problem of maintaining MFA security in computing sessions when the MFA provider is unavailable. (Relevant)

27. **Voice Biometric Authentication Using Machine Learning (WO 2022256595):** This invention manages, trains, and deploys machine learning architectures for voice biometric authentication. (Relevant)

28. **Multi-Factor Authentication in E-Commerce (WO 2023091982):** This invention combines a device-bound identity token, a user-known password, biometric signatures, and a random challenge from a remote authentication system. (Relevant)

29. **User and IoT Device Authentication in Ubiquitous Environments (EP 3373554):** This invention provides a method for user and IoT device authentication in ubiquitous environments. (Relevant)

30. **Biometric Authentication for Enterprise Resources (WO 2000054214):** This invention uses biometric measurements for user authentication, employing a biometric server with defined policies, and

providing flexibility in authentication levels through layering of biometric and non-biometric devices. (Relevant)

31. **Privacy-Preserving Biometric Authentication Using Zero-Knowledge Techniques (EP 4232923):** This invention provides efficient and reliable biometric authentication while maintaining privacy in external-facing scenarios, utilizing zero-knowledge techniques, encryption, and packing techniques to validate biometric templates without leaking sensitive information. (Relevant)

32. **Event-Based User Input Authentication (EP 2732579):** This invention provides an alternative and cost-effective mechanism for dual-factor authentication, addressing the need for enhanced security against stolen or cloned credentials without the high costs associated with biometric readers or the vulnerabilities of keypads. (Relevant)

33. **Multi-Factor or Dynamic Password Authentication (WO 2013019880):** This invention uses a multi-factor password or a dynamic password that varies with parameters like time or location. (Relevant)

34. **Biometric Token-Based Authentication (WO 2020260483):** This invention avoids the exchange of biometric captures or references between devices by using a biometric token, generated by combining a biometric bitstream with reproducible data, to recover a predictable seed of data for authentication. (Relevant)

Unique Components, Devices, Apparatus, Methods, or Systems:

- **Handheld card-device (EP 1925113):** Integrating multiple authentication factors into a single device. (Relevant)
- **Biometric authentication platform system (WO 2016129453):** Managing original biometric data and using majority logic for authentication. (Relevant)
- **Authentication service (WO 2024254315):** Sharing authentication with shared session tokens. (Relevant)
- **External accessory device (EP 4264460):** Performing secure operations when biometric data is insufficient. (Relevant)
- **Biometric token (WO 2020260483):** Generating a token from biometric data to avoid direct biometric data exchange. (Relevant)

- **Deep Neural Network (DNN) for image enhancement (WO 2023107820):** Improving the quality of optical codes for authentication. (Relevant)

Technical Problems Solved and Improvements Provided:

- **Insecure conventional biometric authentication systems:** Solved by privacy-preserving methods using homomorphic encryption (EP 3979552). (Relevant)
- **Weak SMS-based authentication:** Improved by sending multiple codes and requiring user selection (WO 2021212351). (Relevant)
- **Lack of security in legacy applications:** Addressed by providing MFA without rewriting the applications (EP 1841174). (Relevant)
- **Reliance on a single identity provider:** Mitigated by using multiple independent IdPs (WO 2008122108). (Relevant)
- **Compromised digital identity credentials in e-commerce:** Solved by combining multiple authentication factors (WO 2023091982). (Relevant)
- **Cumbersome biometric authentication across devices:** Improved by enabling the sharing of biometric data (EP 4050846). (Relevant)
- **Reduced authentication success rates due to biometric changes:** Addressed by adaptive biometric authentication (EP 2199945). (Relevant)
- **Vulnerabilities in IoT devices:** Solved by providing a method for user and IoT device authentication (EP 3373554). (Relevant)

Applicability and Uses:

The inventions described have a wide range of practical applications and uses, including:

- **E-commerce and Online Banking:** Securely authenticating users for online transactions and account access (EP 3979552, WO 2021026464, WO 2023091982). (Relevant)
- **Physical Access Control:** Controlling access to buildings, facilities, and secure areas (EP 1925113, WO 2023107820, EP 2732579). (Relevant)
- **Mobile Device Security:** Protecting smartphones, tablets, and other mobile devices from unauthorized access (WO 2016099674, WO 2021085799). (Relevant)

- **Enterprise Network Security:** Securing access to company networks and resources (EP 1841174, WO 2000054214). (Relevant)
- **Payment Transactions:** Authenticating users for payment transactions at point-of-sale terminals and online (WO 2016033499, WO 2019133339). (Relevant)
- **Virtual Desktop Environments:** Maintaining MFA security in virtualized desktop environments (WO 2023283499). (Relevant)
- **IoT Device Authentication:** Securing access to and control of IoT devices (EP 3373554). (Relevant)
- **Voice-Based Services:** Providing seamless speaker recognition and voice biometrics-based identification across vendors, devices, and computing services (WO 2022256595). (Relevant)
- **Sharing Data Across Devices:** Accessing data, user accounts, or physical spaces (EP 4050846). (Relevant)

Conclusion:

The patents analyzed in this report showcase a diverse range of innovative approaches to authentication. These inventions address critical challenges in security, privacy, and user experience by leveraging biometric data, multi-factor authentication, cryptographic techniques, and distributed architectures. The solutions presented offer significant improvements over existing authentication methods and have broad applicability across various industries and applications. The ongoing development and refinement of these technologies will play a crucial role in enhancing security and enabling more seamless and user-friendly authentication experiences in the future.

Citations:

- EP 3979552 (Relevant)
- WO 2021212351 (Relevant)
- EP 1841174 (Relevant)
- WO 2008122108 (Relevant)
- WO 2023107820 (Relevant)
- EP 1925113 (Relevant)
- WO 2024254315 (Relevant)
- WO 2009153742 (Relevant)
- WO 2016129453 (Relevant)

- WO 2017083732 (Relevant)
- WO 2016099674 (Relevant)
- WO 2022046181 (Relevant)
- EP 2199945 (Relevant)
- EP 4145312 (Relevant)
- WO 2016145454 (Relevant)
- WO 2016094056 (Relevant)
- WO 2021085799 (Relevant)
- WO 2021026464 (Relevant)
- EP 4050846 (Relevant)
- EP 4264460 (Relevant)
- WO 2013159110 (Relevant)
- EP 2995040 (Relevant)
- WO 2014182787 (Relevant)
- WO 2019133339 (Relevant)
- EP 2560122 (Relevant)
- WO 2016033499 (Relevant)
- WO 2023283499 (Relevant)
- WO 2022256595 (Relevant)
- WO 2023091982 (Relevant)
- EP 3373554 (Relevant)
- WO 2000054214 (Relevant)
- EP 4232923 (Relevant)
- EP 2732579 (Relevant)
- WO 2013019880 (Relevant)
- WO 2020260483 (Relevant)

Contexts: EP 3979552 :: METHOD AND SYSTEM FOR PRIVACY PRESERVING MULTIFACTOR BIOMETRIC AUTHENTICATION\n
WO 2021212351 :: MULTIFACTOR AUTHENTICATION SERVICE\n
EP 1841174 :: Methods and systems for multifactor authentication\n
WO 2008122108 :: REDUNDANT MULTIFACTOR AUTHENTICATION IN AN IDENTITY MANAGEMENT SYSTEM\n
WO 2023107820 :: SYSTEMS AND METHODS FOR ENCRYPTED MULTIFACTOR AUTHENTICATION USING IMAGING DEVICES AND IMAGE ENHANCEMENT\n

EP 1925113 :: SYSTEMS AND METHODS FOR MULTI-FACTOR REMOTE USER AUTHENTICATION\n
WO 2024254315 :: AUTHENTICATION SERVICE WITH SHARED SESSION TOKENS FOR SHARING AUTHENTICATION\n
WO 2009153742 :: IMPROVED BIOMETRIC AUTHENTICATION AND IDENTIFICATION\n
WO 2016129453 :: BIOMETRIC AUTHENTICATION PLATFORM SYSTEM, BIOMETRIC AUTHENTICATION INFORMATION MANAGEMENT DEVICE, BIOMETRIC AUTHENTICATION INFORMATION MANAGEMENT METHOD, AND BIOMETRIC AUTHENTICATION INFORMATION MANAGEMENT PROGRAM\n
WO 2017083732 :: PUBLIC/PRIVATE KEY BIOMETRIC AUTHENTICATION SYSTEM\n
WO 2016099674 :: MANAGING LATENCY AND POWER IN A HETEROGENEOUS DISTRIBUTED BIOMETRIC AUTHENTICATION HARDWARE\n
WO 2022046181 :: BIOMETRIC IDENTIFICATION AND CONTROL SYSTEMS AND METHODS FOR PROVIDING CUSTOMIZABLE SECURITY THROUGH AUTHENTICATION OF BIOSIGNAL REPRESENTATIONS\n
EP 2199945 :: Biometric authentication device and method, computer-readable recording medium recorded with biometric authentication computer program, and computer system\n
EP 4145312 :: INFORMATION PROCESSING APPARATUS HAVING MULTIFACTOR AUTHENTICATION FUNCTION, CONTROL METHOD, AND STORAGE MEDIUM\n
WO 2016145454 :: MULTI-FACTOR USER AUTHENTICATION\n
WO 2016094056 :: MULTIPLE USER BIOMETRIC FOR AUTHENTICATION TO SECURED RESOURCES\n
WO 2021085799 :: ELECTRONIC DEVICE FOR PERFORMING USER AUTHENTICATION BY USING USER BIOMETRIC INFORMATION, AND OPERATION METHOD THEREOF\n
WO 2021026464 :: SYSTEM, METHOD, AND COMPUTER PROGRAM PRODUCT FOR AUTHENTICATING A TRANSACTION BASED ON BEHAVIORAL BIOMETRIC DATA\n
EP 4050846 :: REMOTE USAGE OF LOCALLY STORED BIOMETRIC AUTHENTICATION DATA\n
EP 4264460 :: IMPLEMENTATION OF BIOMETRIC AUTHENTICATION\n
, WO 2016145454 :: MULTI-FACTOR USER AUTHENTICATION\n
WO 2013159110 :: MULTI-FACTOR MOBILE TRANSACTION AUTHENTICATION\n
EP 2995040 :: SYSTEMS AND METHODS FOR HIGH FIDELITY MULTI-MODAL OUT-OF-BAND BIOMETRIC AUTHENTICATION\n
WO 2014182787 :: SYSTEMS AND METHODS FOR HIGH FIDELITY MULTI-MODAL OUT-OF-BAND BIOMETRIC AUTHENTICATION\n
WO 2019133339 :: SYSTEM AND METHOD FOR BIOMETRIC CREDIT BASED ON BLOCKCHAIN\n
EP 2560122 :: Multi-Channel Multi-Factor Authentication\n
WO 2016033499 :: SECURE ON DEVICE CARDHOLDER AUTHENTICATION USNING BIOMETRIC DATA\n
WO 2023283499 :: COMPUTING SESSION MULTI-FACTOR AUTHENTICATION\n
WO 2022256595 :: LIMITING IDENTITY SPACE FOR VOICE BIOMETRIC AUTHENTICATION\n
WO 2016094056 :: MULTIPLE USER BIOMETRIC FOR AUTHENTICATION TO SECURED RESOURCES\n
EP 3979552 :: METHOD AND SYSTEM FOR PRIVACY PRESERVING MULTIFACTOR BIOMETRIC AUTHENTICATION\n
WO 2000054214 :: SYSTEM, METHOD AND COMPUTER PROGRAM PRODUCT FOR ALLOWING ACCESS TO ENTERPRISE RESOURCES USING BIOMETRIC DEVICES\n
EP 4232923 :: VERIFICATION OF BIOMETRIC TEMPLATES FOR PRIVACY PRESERVING AUTHENTICATION\n
WO 2023091982 :: SYSTEMS AND METHODS FOR TRUSTWORTHY ELECTRONIC

AUTHENTICATION USING A COMPUTING DEVICE\n
EP 3373554 :: AUTHENTICATION IN UBIQUITOUS ENVIRONMENT\n
EP 4050846 :: REMOTE USAGE OF LOCALLY STORED BIOMETRIC AUTHENTICATION DATA\n
EP 2732579 :: EVENT DRIVEN SECOND FACTOR CREDENTIAL AUTHENTICATION\n
WO 2013019880 :: METHOD AND APPARATUS FOR USING A MULTI-FACTOR PASSWORD OR A DYNAMIC PASSWORD FOR ENHANCED SECURITY ON A DEVICE\n
WO 2020260483 :: PROVISIONING BIOMETRICS TOKENS\n