You Secure: Passwordless Authentication

Yuzo Iano[1[0000-0002-9843-9761]], Leandro Lima[2[0000-0002-9254-2063]]

and Gabriel Kemmer [3[0009-0032-5544-0353]]

1 FEEC/UNICAMP, Campinas SP, BRA
2 FEEC/UNICAMP, Campinas SP, BRA
3 IBMR, São Paulo SP, BRA
1 yuzo@unicamp.br
2 l140124@dac.unicamp.br
3 gabrielkemmer@k9intelligence.digital

Abstract. Security has been an issue since computers were invented. "How to exchange information securely through the internet" has been one of the most researched topics since the first byte was sent and received. With that in mind, You Secure is a program purely designed to protect you wherever you authenticate. It combines technologies such as FIDO2, cryptography, and blockchain to create more than four layers of protection. The process is distributed across multiple servers, so even if there is a man-in-the-middle attack, your credentials would not be compromised. The system is designed to use your cellphone or notebook to generate private and public keys, linked to facial and biometric identification. Blockchain is used to store part of your data, enabling decentralized validation, with separate servers managing all of these security protocols, providing ultimate security for the user.

Keywords: Keywords—security; authentication; passwordless; blockchain; cryptography; decentralized authentication; multi-factor authentication (MFA); biometric authentication; public-key infrastructure (PKI); man-in-the-middle protection; WebAuthn; device-based authentication; encryption; privacy

1 Introduction

1.1 The Evolution of Password Security

To begin our adventure through the You Secure system, we need to take a journey back in time to understand how password security has evolved. The story starts in the 1960s, where passwords were stored in plaintext—meaning anyone with access to the system could see the password without any protection. This primitive method of securing user credentials was quickly identified as a major vulnerability. As a

response, the 1970s introduced basic encryption with the Data Encryption Standard (DES). This encrypted passwords before saving them in directories like /etc/passwd and, later on, /etc/shadow, offering the first significant step toward protecting passwords from unauthorized access.

Moving into the 1980s, hashing algorithms like MD5 (Message Digest Algorithm) were introduced. Hashing, unlike encryption, is a one-way process: a hash cannot be "decrypted" back into its original form, making it harder for attackers to retrieve the original password [1]. By the 1990s, we saw the introduction of Secure Socket Layer (SSL) and Transport Layer Security (TLS), which allowed passwords to be transmitted securely over the network by encrypting the communication between the user and the server. Around the mid-90s, security measures advanced further with the adoption of salted hashes. Salting added a random value to the password before hashing, ensuring that even if two users had the same password, their hashes would look different. This innovation was a direct response to hackers using rainbow tables—precomputed databases of hashes used to crack passwords through brute-force attacks [2].

1.2 **Advances in Modern Authentication Methods**

With the arrival of the new millennium, security experts focused on making hacking attempts increasingly costly and time-consuming. New password hashing algorithms like bcrypt, PBKDF2, and scrypt were developed. These algorithms incorporated both salting and key stretching techniques, which slow down brute-force attacks by increasing the computational effort required to guess passwords, thereby enhancing security [3].

Despite these advances, the vulnerabilities of password-based security persisted, leading to the development of two-factor authentication (2FA). Introduced in the 2000s, 2FA added an extra layer of security by requiring not just a password but a second authentication factor, such as a one-time code sent to a mobile device. In 2006, OAuth became widely used, allowing users to authenticate using credentials from a third-party provider, which introduced a new level of convenience and security [4]. Between 2010 and 2020, passwordless methods like biometrics (fingerprints and facial recognition), magic links, and WebAuthn emerged as innovative approaches to authentication. Today, advanced technologies such as Federated Identity and Decentralized Authentication, often using blockchain or WebAuthn, represent the cutting-edge in user authentication and identity management [5].

It's also important to distinguish WebAuthn from FIDO2. FIDO2 consists of two main components: the WebAuthn API and a Client Authenticator. Together, they enable passwordless login experiences across web browsers and devices. WebAuthn is backward-compatible with earlier FIDO U2F (Universal 2nd Factor) authenticators, which were often hardware-based, such as bitcoin wallets or YubiKeys. The CTAP1 protocol ensures that these older FIDO U2F Security Keys remain useful as a second factor in authentication when combined with modern WebAuthn-compatible services [6].

1.3 The Role of You Secure in Modern Security

Despite all these advancements, the battle for better security is never over, which is why You Secure exists. The system addresses modern security challenges by integrating three cutting-edge technologies: FIDO2 for passwordless user authentication, advanced cryptographic methods for data security, and blockchain for decentralized credential verification. By combining these technologies, You Secure creates a multi-layered security framework that ensures the highest level of protection for user credentials and sensitive information. Each technology complements the others, providing a comprehensive defense against the ever-evolving threats in today's digital landscape.

2 FIDO2: The Foundation of Secure Authentication

FIDO2 is the foundation of the authentication process. By leveraging a combination of the WebAuthn and CTAP protocols, You Secure enables passwordless login using public-key cryptography. Users register their devices (e.g., smartphones, laptops) as authenticators, where the device generates a public-private key pair. The private key remains securely on the user's device, while the public key is shared with the server. This approach eliminates the risks associated with password-based systems, such as phishing and credential reuse attacks [7][8][9].

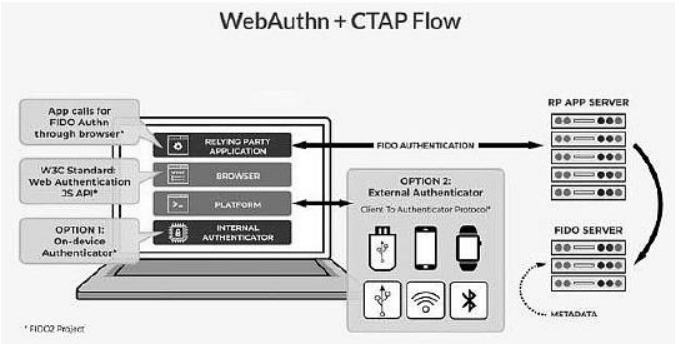

Fig.1. WebAuthn flow

To generate the public-private key pair, the You Secure system uses relying party information, which is the entity (such as a website or service) requesting authentication. The public-private key pair is bound to the specific domain or service requesting the authentication. This ensures that the keys cannot be used by anyone or any other service, as they are associated solely with the You Secure system [10].

Once the key pair is generated, a challenge—a unique cryptographic number—is created by the server for each authentication attempt, as shown on Fig.1. This challenge guarantees that each login attempt is unique, preventing replay attacks where attackers might try to reuse previous authentication data [11][12].

During the login process:

1. The user receives the challenge and other metadata like the relying party information.
2. The user's device checks that the relying party matches the service it’s registered for.
3. The user's device signs the challenge using the private key, which is securely stored on the device (e.g., smartphone or hardware security key).
4. The signed challenge is then sent back to the server. The server uses the public key associated with the user to verify the signature. If the signature is valid and matches the public key and original challenge, the server permits the user to log in [13][14].

To enhance security further, You Secure stores the public key on a blockchain, ensuring that even if the server is compromised, the public key cannot be altered or leaked. During login attempts, the public key is securely retrieved from the blockchain only when needed to verify the user’s signed challenge [15].

Beyond the foundational FIDO2 protocols, You Secure integrates several advanced features to enhance both security and usability. One of these key features is the integration of biometrics, such as fingerprint scanners or facial recognition, as a seamless authentication method. Biometrics ensure that only the registered user can unlock the private key, adding a second layer of protection. This method not only improves user experience by providing fast and intuitive logins but also strengthens security by requiring something the user is, in addition to something they possess (the private key on their device) [16][17].

2.1 Multi-Device Support and Cross-Platform Compatibility

You Secure also supports multi-device authentication, allowing users to register multiple devices as authenticators, including one device as administrator device. This capability is critical for ensuring that users can still access their accounts if they lose or upgrade their primary device. The system maintains separate public-private key pairs for each registered device, ensuring that no device can be used as a fallback unless it's explicitly trusted by the user [18]. Furthermore, by leveraging the WebAuthn API, You Secure is compatible across major web browsers and platforms, including desktop and mobile operating systems, providing users with flexibility and a consistent login experience regardless of the device or system they are using [19].

2.2 Privacy Considerations and Anonymity

FIDO2 and WebAuthn also prioritize user privacy. No sensitive personal information, such as usernames or biometrics, is stored or transmitted during the authentication process. The server only stores public keys, which do not reveal any information about the user or the device. Moreover, each authentication session is tied to a unique cryptographic challenge, further reducing the risk of tracking users across different

services or platforms. This emphasis on privacy ensures that users retain control over their data while benefiting from robust security features [20].

2.3 Decentralized Identity and Blockchain Integration

Looking forward, You Secure is exploring integration with decentralized identity systems. These systems allow users to have complete control over their digital identities by using blockchain to manage authentication data. Decentralized identities remove the need for centralized servers, which are often vulnerable to attacks. Instead, users manage their own credentials and decide which services or websites can access them. This shift toward decentralized identity aligns with You Secure's mission to provide secure, privacy-focused, and user-centric authentication solutions [21][22].

Blockchain technology, as utilized by You Secure to store public keys, also ensures transparency and immutability. Since blockchain is a distributed ledger, any attempt to modify or tamper with the stored public keys would be easily detected. Additionally, because blockchain is decentralized, it eliminates the need for trust in a single centralized authority, thereby mitigating the risks of centralized server failures or compromises [23]. This ensures the integrity of the public key infrastructure even in the event of server-side vulnerabilities.

2.4 Resistance to Advanced Threats

You Secure offers robust protection against advanced threats, including man-in-the-middle (MitM) attacks, phishing, and credential stuffing. Since users are not required to share or enter passwords, common attack vectors such as phishing emails or malicious websites designed to steal passwords become ineffective. Furthermore, the challenge-response mechanism used during authentication makes it extremely difficult for attackers to intercept and replay authentication attempts, even if they manage to compromise a network [24].

You Secure also leverages hardware-backed security features like Trusted Platform Module (TPM) and Secure Enclave technologies, where available, to ensure that private keys are stored in isolated, tamper-resistant environments on the user's device. These hardware-backed systems provide additional protection against physical tampering and software-based attacks, further securing the authentication process [25].

By combining FIDO2 protocols, biometric authentication, blockchain technology, and advanced hardware security measures, You Secure delivers a robust, scalable, and user-friendly passwordless authentication solution. As the landscape of cybersecurity continues to evolve, You Secure remains committed to pushing the boundaries of secure authentication, ensuring that users are protected from both present and emerging threats.

3 Cryptography

The system is capable of allowing authentication on servers, websites, e-commerce platforms, and securing credit card information during online shopping. To handle this, in addition to FIDO2, cryptographic methods further enhance security by encrypting sensitive user data. For example, in the backend system of You Secure, encryption algorithms such as Fernet encryption ensure that sensitive information, such as credit card details, is stored securely. This ensures that even if an attacker gains unauthorized access to the data, they will not be able to decipher it without the corresponding decryption key [26][27].

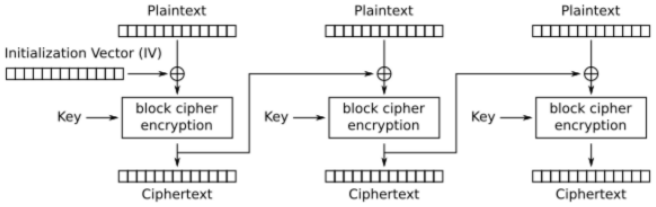

Fig.2. Cipher Block Chaining (CBC) mode decryption

Fernet encryption uses a 256-bit symmetric key encoded in base 64 to encrypt and decrypt the data. The encryption uses a random 128-bit initialization vector (IV), which is applied in Cipher Block Chaining (CBC) mode, as shown on Fig.2. The purpose of this method is to ensure that the message is encrypted multiple times, with the randomness of the IV preventing detectable patterns. Each plaintext block is XOR-ed with the previous ciphertext block before being encrypted. This creates a dependency between blocks, making the encryption stronger [28][29][30].

4 Blockchain

To safeguard user credentials and verification data in a decentralized and tamper-resistant manner, blockchain technology is utilized. Specifically, You Secure leverages the blockchain to store hashed public keys and other metadata, creating an immutable, decentralized ledger of verification data. This decentralized verification method provides an additional layer of trust and integrity, as blockchain ensures that data cannot be altered or forged. The blockchain acts as a trusted third party that validates device authenticity without relying on a centralized authority, thereby reducing the risk of single points of failure. [31][32][33]

To authenticate the ciphertext, the system uses HMAC (Hash-based Message Authentication Code) as shown on Fig 3, which combines a cryptographic hash function with a secret key to verify the integrity of the ciphertext and ensure it has not been tampered with or altered.[34]

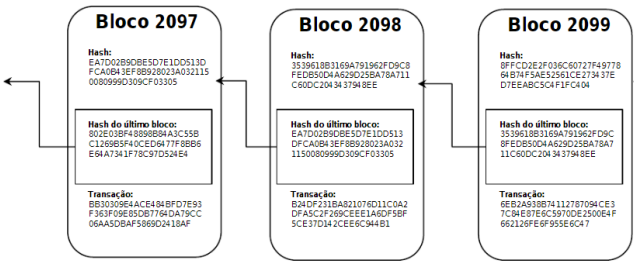

Fig.3. Hash-based Message Authentication Code

5 Other Layers Of Security

You Secure employs multiple additional layers of security throughout the authentication process, significantly enhancing the overall integrity and safety of user interactions. One of the critical features of this system is the use of sessions to uniquely identify each user. By establishing secure sessions, You Secure can maintain user state and store essential information directly within the user's browser, ensuring that data remains accessible only to authenticated individuals. This session management not only streamlines the user experience but also adds an extra barrier against unauthorized access.

To further bolster security during data transmission, You Secure utilizes CBOR (Concise Binary Object Representation). This technology is employed to compact and encode transmitted data efficiently, reducing the size of the data being sent while maintaining its integrity. By using CBOR, the system optimizes bandwidth and speeds up the communication process, making it both efficient and secure. This encoding method minimizes the chances of data corruption or manipulation during transmission, adding yet another layer of protection.[35][36]

In addition, the system incorporates buffer-to-base64 encoding to securely encrypt data before it is transmitted. This method ensures that the information being sent is transformed into a format that is not only compact but also resistant to unauthorized access. By encrypting data in this way, You Secure effectively safeguards sensitive information from potential interception by malicious actors, ensuring that user data remains confidential and secure.[35]

Lastly, the integration of BigNumber.js plays a crucial role in maintaining precision in cryptographic operations. Cryptography often involves mathematical calculations that require a high degree of accuracy, and BigNumber.js provides the necessary tools to handle large numerical values with precision. This is essential in cryptographic contexts, where even the smallest error can compromise security. By ensuring accuracy in these operations, You Secure enhances the reliability of its security

measures, ultimately creating a more robust authentication process that protects users' identities and sensitive information effectively.

6 Results

The outcome of the system is security, anonymity, and authentication on any server for each user of You Secure. The system is capable of preventing the following attacks (among others):

- **Phishing attacks**: In phishing attacks, hackers trick users into revealing credentials by impersonating a legitimate service. With You Secure, public key cryptography and the relying party mechanism prevent credentials from being accepted on unauthorized servers, ensuring security.

- **Credential Stuffing**: In credential stuffing, attackers steal usernames and passwords used on other services and attempt to use them in the system. However, with You Secure, the user does not have a password. Authentication is performed using public-private key pairs, rendering this attack ineffective.

- **Man-in-the-Middle (MitM) attacks**: In these attacks, an attacker intercepts communication between the client and server to steal credentials. With cryptographic signatures, challenges, and the relying party mechanism, the attacker will not gain any useful information because the user’s private key remains securely stored on the user’s device.

- **Replay attacks**: In a replay attack, an attacker captures legitimate authentication data and reuses it to gain unauthorized access. You Secure uses a challenge-response model, where each authentication request involves a new cryptographic challenge generated by the server, preventing reuse of previous data.

- **Brute Force attacks**: Brute force attacks involve systematically guessing passwords or cryptographic keys by trying all possible combinations. The complexity and length of the cryptographic keys used by You Secure make brute force attacks computationally impractical

7 Conclusion

By combining these three cutting-edge technologies—FIDO2, cryptography, and blockchain—the You Secure system establishes a comprehensive and multi-layered

approach to security that addresses the complexities of the modern digital landscape. In an age where cyber threats are evolving rapidly, it is crucial to adopt strategies that are not only effective but also user-friendly. The integration of these technologies allows for a robust security framework that caters to the needs of users while safeguarding their sensitive information.

You Secure provides a foundation for secure, decentralized authentication by enabling passwordless access. This technology eliminates the risks associated with traditional passwords, which are often vulnerable to theft and compromise. By using strong authentication methods, such as biometrics or security keys, You Secure ensures that only authorized users can access their accounts. This layer of security significantly reduces the chances of unauthorized access, making it a vital component of the You Secure system.

Cryptography further enhances this security model by encrypting user data, ensuring that sensitive information remains protected during transmission and storage. By employing advanced cryptographic techniques, the system can safeguard against interception and unauthorized access. This means that even if data is compromised, it remains unreadable to malicious actors. The combination of FIDO2 and cryptography creates a fortified barrier against cyber threats, providing users with peace of mind.

Blockchain technology plays a pivotal role in ensuring the integrity and transparency of the authentication process. Its decentralized nature means that user data is not stored in a single location, making it much harder for hackers to target. This innovative integration not only enhances security but also fosters a seamless, passwordless user experience. Ultimately, You Secure provides the highest level of protection for user data and identities, enabling individuals to navigate their online activities with confidence and paving the way for a safer digital future. This comprehensive strategy positions the You Secure system as a leader in the ongoing battle against cyber threats, ensuring that users can engage with digital platforms securely and without compromising their privacy.

References

1. "Password Hashing: Your Security Staple", Mojoauth.com, 2024.
2. "The Evolution of Password Hashing", Psono.com.
3. "About Secure Password Hashing", Blog Security Overflow
4. "Bcrypt and a Short History of Password Hashing", The New Stack.
5. "History of Cryptography", Wikipedia.
6. "Password Storage Cheat Sheet", OWASP.org.
7. "FIDO2: Web Authentication (WebAuthn)", fidoalliance.org
8. "FIDO2, CTAP, and WebAuthn - Identity Hub", Transmit Security.
9. "What Is FIDO2?" Microsoft Security.
10. "Learning FIDO2, WebAuthentication, and CTAP? Start here", Goteleport.com.
11. "FIDO2 - FIDO Alliance", Fidoalliance.org.
12. "What are passkeys?", Passkey.dev.

13. "What Is FIDO2?" Microsoft Security.
14. "What is CTAP?", Youbico.com
15. "FIDO2 - FIDO Alliance", Fidoalliance.org.
16. "FIDO2 + Biometrics – A Logical Approach to Secure Unified Authentication for Hybrid Working," Fingerprints.com.
17. "An Introduction to FIDO2 for Biometric Authentication," NordicAPIs.com.
18. "FIDO2: Multi-Device Authentication and Flexibility," Yubico.com.
19. "WebAuthn API – Seamless Integration Across Platforms," Fidoalliance.org.
20. "How FIDO2 and WebAuthn Protect User Privacy," Fidoalliance.org.
21. "Decentralized Identity and Blockchain: The Future of Authentication," Microsoft.com.
22. "Blockchain for Decentralized Identity," IBM.com.
23. "How Blockchain Ensures Security and Transparency in Public Key Infrastructure," Deloitte.com.
24. "How FIDO2 Prevents Phishing and MitM Attacks," Yubico.com..
25. "TPM and Secure Enclave: Hardware Security in FIDO2 Authentication," Apple.com..
26. "Fernet (symmetric encryption) — Cryptography Documentation", Cryptography.io.
27. "What is Fernet and when should you use it?", Comparitech.com.
28. "Why You Should Use AES 256 Encryption to Secure Your Data" Progress.com
29. "Block Cipher modes of Operation", Geeksforgeeks.com.
30. "Cipher block chaining (CBC)", Techtarget.com.
31. "A Blockchain-Based Decentralized Public Key Infrastructure for Information-Centric Networks", MDPI.com
32. "Use Cases: Blockchain for Public Records and Identity Verification", BlockApps Inc.
33. "Blockchain Authentication | Overview, How It Works, Factors", FinanceStrategists.com
34. "How HMAC Works", Okta.com
35. "Extensible Binary Encoding with CBOR", Endpointdev.com.
36. "CborTree", Github.com.