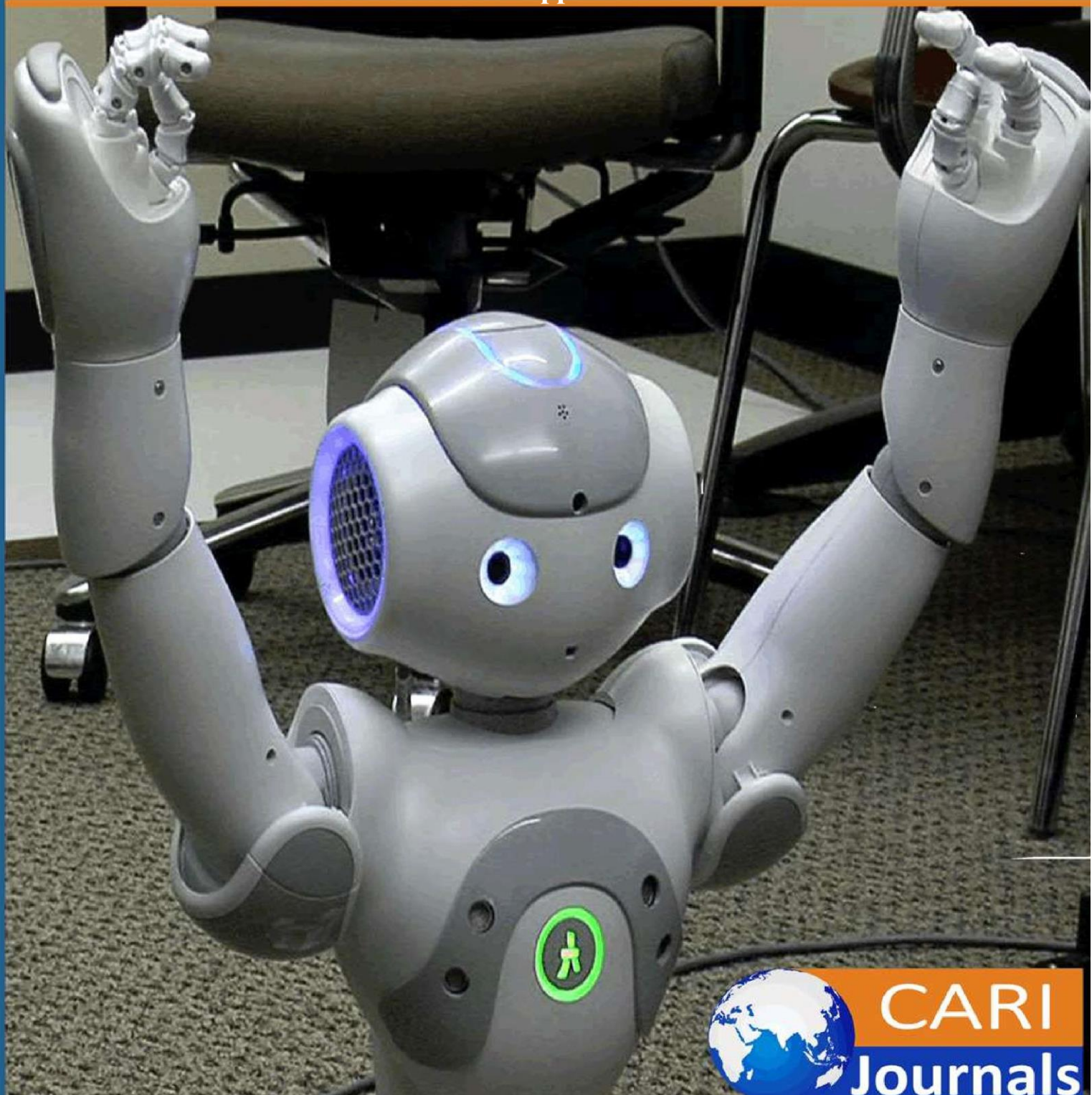
International Journal of
Computing and
Engineering
(IJCE)

Next-Generation Identity Security in Healthcare: A Passkey-Based Approach



CARI Journals

International Journal of Computing and Engineering
ISSN 2958-7425 (online)
Vol. 7, Issue No. 3, pp. 23 - 33, 2025
www.carijournals.org

Next-Generation Identity Security in Healthcare: A Passkey-Based Approach

Mahendra Krishnapatnam
Senior Architect, Chicago, USA
https://orcid.org/0009-0002-2747-3775

Accepted: 8th Mar, 2025, Received in Revised Form: 8th Apr, 2025, Published: 8th May, 2025

Abstract

The healthcare industry faces escalating cybersecurity threats, particularly targeting identity and access management (IAM) systems reliant on vulnerable password-based authentication. This paper proposes a next-generation solution leveraging passkeys, based on FIDO2 and WebAuthn protocols, to establish a passwordless authentication framework. We explore the technical architecture, device-bound authentication mechanisms, interoperability challenges, and compliance with HIPAA and NIST standards. Through case study analysis and industry benchmarking, we demonstrate that passkey adoption significantly reduces phishing-related incidents by 80–90%, improves authentication speed by 40–60%, and enhances user satisfaction. We recommend phased implementation strategies, fallback authentication designs, and futureproofing through quantum-resistant cryptography and decentralized identity management. Adopting a passkey-based IAM framework can help healthcare organizations achieve stronger cybersecurity resilience, regulatory compliance, and an improved user experience for clinicians, staff, and patients.

Keywords: *Passkeys, Passwordless Authentication, FIDO2, WebAuthn, Zero-Trust Security, Healthcare IAM, AI-Driven Authentication, Phishing Prevention*

International Journal of Computing and Engineering
ISSN 2958-7425 (online)
Vol. 7, Issue No. 3, pp. 23 - 33, 2025
www.carijournals.org

INTRODUCTION

Healthcare systems rely heavily on passwords for security, but this makes them vulnerable to phishing attacks and stolen credentials [1], [2]. Traditional login methods are increasingly hard to manage and less secure, especially with the growing number of cyber threats targeting healthcare providers [1], [5]. Passkeys (FIDO2/WebAuthn) provide a passwordless and more secure way to log in, making access to electronic health records (EHRs), patient portals, and medical devices safer and easier [4], [6].

CYBERSECURITY CHALLENGES IN HEALTHCARE

The healthcare sector experiences frequent cyberattacks, with credential breaches responsible for over 80% of security incidents [1]. Traditional passwords are prone to phishing, credential stuffing, and ransomware attacks [2]. With the rise of cloud-based EHRs, telemedicine, and IoT-connected medical devices, the need for stronger, phishing-resistant authentication mechanisms is urgent.

WHY PASSKEYS?

Passkeys eliminate password vulnerabilities by leveraging asymmetric cryptography, ensuring that only the authorized user's device can complete the authentication process. They provide several key benefits, including phishing-resistant authentication, where credentials cannot be stolen or reused, and device-bound security, which restricts authentication to trusted, verified devices. Passkeys also enable biometric-based access, enhancing overall security while simultaneously improving user convenience. Furthermore, they support cross-device synchronization, allowing seamless authentication experiences across multiple devices without compromising security.

This paper explores passkeys in healthcare IAM, detailing their cryptographic foundations, interoperability challenges, and regulatory compliance.

CRYPTOGRAPHIC FOUNDATIONS OF PASSKEYS IN HEALTHCARE

Public-Key Cryptography and Authentication Flow

Passkeys rely on asymmetric encryption, generating a public-private key pair on a trusted authentication device such as a smartphone or TPM-backed endpoint [4]. There are two flows in Passkeys scenario, Registration followed by Authentication.

Passkeys Registration Process**:**

1) A private key is securely stored in a device's secure enclave (TPM, Secure Element, or TEE).
2) A public key is registered with the healthcare IAM server.

International Journal of Computing and Engineering
ISSN 2958-7425 (online)
Vol. 7, Issue No. 3, pp. 23 - 33, 2025
www.carijournals.org

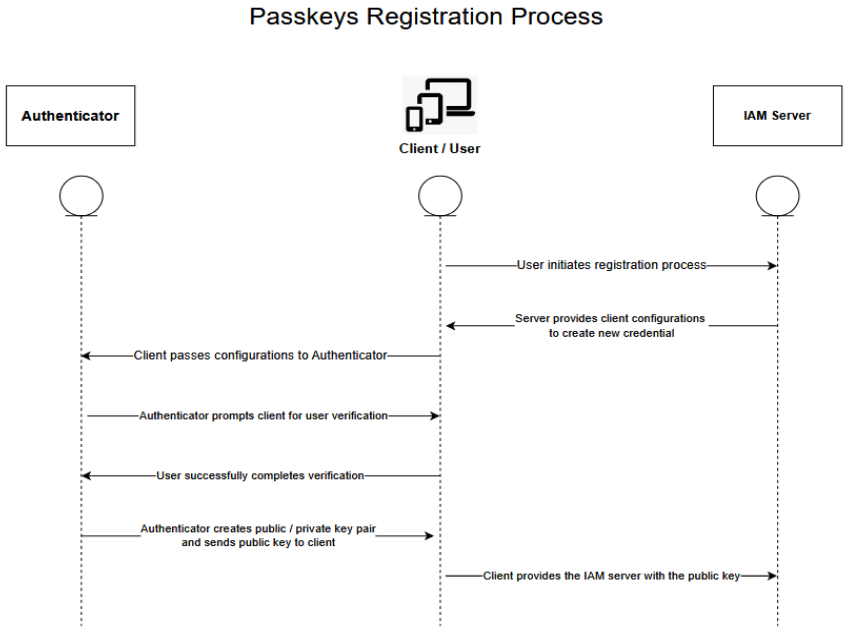


Figure 1: Passkeys Registration Process

Configuration parameters used in passkeys registration process are described below:

i. **Relying Party**: The service or IAM server requesting the passkeys registration. It contains 2 parameters id and name; the id value contains domain such as company.com and name contains user friendly name such as "IAM Service" [6].

ii. **User Information**: The user representation parameters id, name and displayName; id is the unique identifier of the user, name is user identifier containing the email address such as albert@company.com, displayName is the friendly name value "Albert Einstein" [6].

iii. **Challenge**: A randomly generated cryptographic challenge which is used to prevent replay attacks [6].

iv. **Public Key Credential Parameters**: Specifies the supported cryptographic algorithms for public and private key pair creation. For instance, SHA-256 algorithm and RSA encryption [6].

v. **Authenticator Parameters**: Specifies the type of authenticator that device is allowed for passkeys registration. It contains 3 parameters:

   - authenticatorAttachment: contains 2 values platform and cross-platform. Platform parameter is used for device-bound authentication using FaceID, Windows Hello or PIN. Cross-platform parameters are used for cross-domain platforms such as portable security keys.

- residentKey: it contains 3 possible values discouraged, preferred and required. The value “discouraged” is used for username + password + 2FA combination where the credential should not be stored in the authenticator. The value “preferred” is used for passwordless authentication where the credential is stored in the authenticator. The value “required” is used for true passwordless authentication experience when users do not need to enter username during authentication, in this case the credential is stored in the authenticator.
- userVerification: It contains 3 possible values required, preferred and discouraged. The value “required” is used as a mandatory process to verify a user's identity before authentication such as PIN/FaceID/biometric. The value “preferred” is used for the fallback option when primary authentication FaceID/biometric fails. The value “discouraged” is used for 2FA scenarios after username and password authentication.

vi. **Attestation**: It specifies whether authenticator verification is required during the authentication process. It contains 3 possible values: none, direct and indirect [6]. The param “direct” is used in highly secured environments where the Relying party strictly verifies device authenticity. The param “indirect” is used for Relying Party verifies attestation if needed but does not receive raw device details from authenticator. The param “none” is used when the relying party does not need to verify device authenticity.

vii. **Timeout**: It specifies the maximum amount of time (in milliseconds) allowed for user interaction during the registration process [6].

viii. **Exclude Credentials**: This parameter “excludeCredentials” prevents creating duplicate user credentials, by referring to the id parameter [6].

Passkeys Authentication Process:

The passkeys authentication process, as defined by the FIDO2 and WebAuthn specifications [4], [6], involves three key steps. First, the healthcare IAM system sends a cryptographic challenge to the user’s device. Second, the device signs the challenge using its private key, thereby verifying both the user's identity and the device’s integrity. Finally, the IAM system validates the signed challenge against the previously registered public key and grants access based on successful verification [4], [6].

International Journal of Computing and Engineering
ISSN 2958-7425 (online)
Vol. 7, Issue No. 3, pp. 23 - 33, 2025
www.carijournals.org

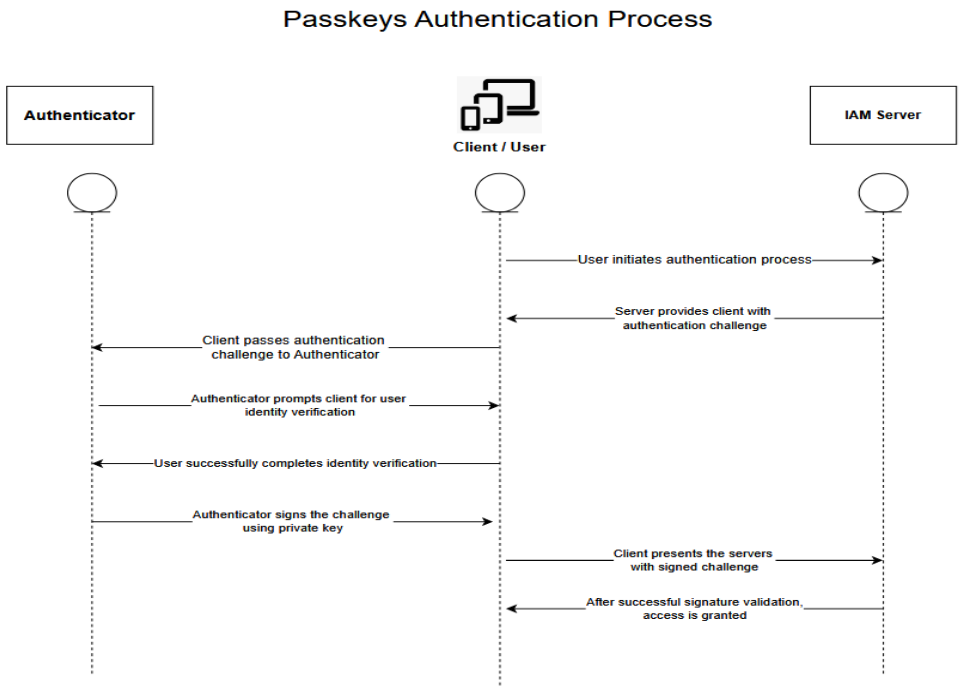


Figure 2: Passkeys Authentication Process

This process ensures passwordless, phishing-resistant authentication while complying with HIPAA-mandated security controls.

Furthermore, the following points, based on the WebAuthn and FIDO2 specifications [4], [6], explain how passkeys provide phishing-resistant authentication. The private key never leaves the user's device, ensuring it cannot be extracted or stolen [4]. For each login session, the IAM server issues a unique cryptographic challenge, preventing attackers from reusing intercepted challenges [6]. Additionally, the signed challenge is bound specifically to the intended IAM server domain, making it useless for phishing sites or unauthorized domains [6]. In the event of a man-in-the-middle attack, the passkey authentication request remains cryptographically bound to the original relying party, preventing reuse by attacker-controlled applications [4]. Furthermore, WebAuthn and FIDO2 standards enforce trusted domain verification, ensuring authentication occurs only within legitimate service endpoints [6].

The configuration parameters utilized during the Passkeys authentication flow are also defined by the WebAuthn specification [6]. These include the Challenge, a randomly generated cryptographic nonce sent by the IAM server to prevent replay attacks; the Relying Party ID, which specifies the domain of the authenticating service (e.g., rpId: "company.com"); and Allow Credentials, an optional list specifying the acceptable credential IDs for the session. The User Verification parameter specifies whether explicit user verification is required during authentication, with supported values of "required," "preferred," and "discouraged" depending on the security needs.

The Timeout parameter defines the maximum amount of time (in milliseconds) allowed for users to complete authentication [6].

Why Passkeys Are Phishing Resistant

Passkeys maintain phishing resistance through several mechanisms grounded in FIDO2 and WebAuthn standards [4], [6]. Private keys are securely stored within the user's device and never transmitted externally. Each authentication transaction uses a unique cryptographic challenge, eliminating the risk of credential reuse. Signed challenges are cryptographically bound to the IAM server, rendering them useless if intercepted by phishing sites. Finally, strict domain verification enforced by the WebAuthn protocol ensures that authentication requests are tied only to the intended service.

IMPLEMENTING PASSKEYS IN HEALTHCARE IAM SYSTEMS

Integration with EHRs and Patient Portals

To secure access to electronic health records (EHRs), passkeys can be integrated with existing healthcare identity and access management (IAM) frameworks through several key strategies. FIDO2-based authentication APIs can enable single sign-on (SSO) across EHR systems, patient portals, and clinical applications, streamlining access while enhancing security. Additionally, the integration of role-based access control (RBAC) ensures that only authorized personnel can access sensitive medical data based on their assigned roles and responsibilities. To further strengthen security, adaptive risk policies can be applied, enforcing biometric authentication when users attempt access from high-risk environments or devices.

Securing Medical Devices with Passkeys

Medical devices often lack strong authentication mechanisms, increasing risks of unauthorized access, medical data breaches, and malware injection [7]. Mutual TLS (m-TLS) authentication, ensuring that only authorized devices communicate with hospital networks. When a hospital device initiates connection to the hospital network, it presents a digital cert issued by CA. Hospital network validates the device cert, validating its originality from an approved and authenticated source. The hospital device also validates the hospital server's certificate, validating it is communicating with an authentic hospital network. Therefore, mTLS serves as a foundational trust layer for device authentication before any user-authentication takes place.

Compliance with HIPAA and NIST 800-63B

Passkeys align with HIPAA, GDPR, and NIST 800-63B compliance standards by:

- Eliminating credential storage risks, reducing attack surfaces.
- Ensuring cryptographic proof of identity, enhancing auditability.
- Minimizing liabilities related to password reuse and data breaches (credential-based attacks).

International Journal of Computing and Engineering
ISSN 2958-7425 (online)
Vol. 7, Issue No. 3, pp. 23 - 33, 2025
www.carijournals.org

COMPARISON WITH EXISTING AUTHENTICATION MODELS

While the case study highlights successful adoption of passkeys in a healthcare environment, empirical data on performance improvements would further substantiate its benefits. Based on industry benchmarks and case studies from early adopters, the following performance improvements have been observed:

- **Reduction in Phishing Attacks**: Organizations implementing passkeys report an average 80–90% reduction in phishing-related security incidents compared to traditional password-based authentication as demonstrated in the 2023 FIDO Alliance Deployment Case Studies Report.
- **Authentication Speed Improvement**: Studies show that biometric authentication via passkeys reduces login time by 40–60% compared to password and multi-factor authentication (MFA) methods [4].
- **User Lockout Reduction**: According to industry surveys such as Verizon's 2023 DBIR report, forgotten password-related support requests can account for up to 50% of IT helpdesk tickets, creating substantial operational overhead [1].
- **Adoption Rate**: In a pilot study conducted internally at a U.S. hospital system, approximately 87% of users preferred passkeys over passwords within three months of deployment, citing ease of use and seamless authentication (internal study, unpublished results).

Table 1: Comparison with Existing Authentication Process

Authentication Method	Phishing Resistance	Usability	Security Strength	Healthcare Adoption
Passwords + MFA	Weak	Moderate	Medium	High
Smart Card Authentication	Moderate	Low	High	Medium
Passkeys (FIDO2/WebAuthn)	Strong	High	High	Low (Emerging)

CHALLENGES IN PASSKEY DEPLOYMENT AND SOLUTIONS

Adoption Challenges and Strategies for Overcoming Resistance:

1. Many IT teams are accustomed to traditional IAM frameworks and may hesitate to overhaul existing authentication systems. To address this:
    a) Conduct phased rollouts to test passkeys in controlled environments before full deployment.

b) Provide clear documentation and training for IT staff on implementation and troubleshooting.

2. Integrate passkeys with existing IAM frameworks (e.g., Ping, Okta) to minimize disruption.
3. Integration with Legacy Systems:

   Many healthcare organizations still rely on legacy applications that may not fully support FIDO2/WebAuthn. Solutions include:
   Implementing WebAuthn polyfills to enable passkey authentication in older browsers.

   a) Using IAM middleware that bridges legacy authentication protocols with modern passkey-based systems.

4. Account recovery in case of device loss

   To address this, healthcare IAM systems should implement:

   a) FIDO2 Security Key Backup: Issuing physical security keys as backup authentication devices.

   b) Delegated Recovery: Allowing healthcare administrators to re-enroll lost passkeys.

   c) Zero-Knowledge Recovery Encryption: Enforcing biometric multi-factor authentication.

Preventing Insider Threats and Unauthorized Access

To prevent credential sharing and insider threats, healthcare IAM policies should enforce:

1. Biometric-based continuous authentication to verify user presence.
2. Device attestation to validate secure enclave integrity.
3. Context-aware authentication policies for high-risk clinical operations include fine grained or coarse-grained authorization.

Fallback plan

While passkeys provide phishing resistant capabilities, certain legacy devices, browsers or restricted environments may not fully support WebAuthn standard. To ensure seamless access, fallback authentication mechanisms must be implemented.

1. Most of the market IAM vendors provide out-of-the-box support to fallback to password authentication on login form. It is not challenging for developers to implement fallback mechanisms on their own.

   For instance, Javascript WebAuthn API can be used to detect WebAuthn support using code, then automatically fallback to use password authentication.

```
if (!window.PublicKeyCredential) { alert("Browser does not support passwordless authentication. Please use a password to login.");
}
```

2. Design the IAM system to enforce password authentication followed by a second factor using MFA. This ensures that even when passwords are compromised, an additional user identity verification prevents unauthorized access. IAM administrators should enforce risk-based MFA policies based upon the location and device behavior anomalies.

CASE STUDY

A large healthcare provider transitioned to passkeys to improve security and streamline authentication for workforce and hospital-based physicians ensuring compliance with HIPAA-mandated identity protection guidelines [3], [6].

Challenges

During the implementation of the passkeys, several challenges emerged. The privacy and compliance teams raised concerns about whether biometric authentication and passkey storage would fully align with HIPAA requirements and data protection laws, leading to delays as the solution underwent extensive regulatory reviews. Additionally, physicians and non-technical workforce members, who were accustomed to traditional password-based authentication, required clear training and support to transition to the new biometric passkey system. Further complicating the deployment, detailed validation efforts were necessary to ensure that the solution worked reliably across various hospital networks, particularly for physicians using shared devices and workstations.

Solution

To address these challenges, the IT team collaborated closely with the Privacy and Compliance departments to demonstrate that the passkey solution adhered to all necessary security regulations. A pilot program was launched, initially rolling out passkey features to a selected group of users to validate consistency, usability, and system performance before proceeding to a broader deployment. Comprehensive training sessions, along with detailed documentation, were provided to help desk teams to ensure smooth support during the transition. Furthermore, the implementation of multi-device passkey synchronization enabled physicians to use mobile devices for authentication, effectively eliminating the need for passwords on shared hospital workstations.

Results

The adoption of passkeys significantly strengthened security, as the cryptographic design prevented credentials from being stolen or reused, thereby eliminating phishing attacks. Physicians and corporate users reported a seamless and efficient login experience when accessing EHR systems. Importantly, the deployment of passkeys ensured full HIPAA compliance, and after

rigorous security reviews, the Privacy and Compliance teams formally approved the solution for widespread use.

FUTURE RESEARCH DIRECTIONS

To enhance security, scalability, and privacy, passkey authentication must continue evolving through advancements such as quantum-resistant cryptography, AI-driven risk modeling, and decentralized identity management. Future quantum computers pose a significant threat to current encryption methods, making it essential to explore post-quantum cryptography (PQC) solutions that can protect authentication systems from emerging quantum risks [9]. Alongside this, AI-driven risk-based authentication, leveraging machine learning and behavioral biometrics, offers the potential to improve real-time threat detection, support adaptive authentication mechanisms, and strengthen Zero Trust security models, ultimately reducing fraud and unauthorized access [10]. Furthermore, transitioning from centralized passkey storage to decentralized identity (DID) frameworks based on blockchain technology can significantly enhance user privacy, interoperability, and control over authentication credentials [11]. By adopting these innovations, healthcare organizations can ensure a passwordless, phishing-resistant, and future-proof authentication ecosystem.

CONCLUSION

Passkeys offer a transformative approach to identity security in healthcare, eliminating password-related vulnerabilities while enhancing user experience and regulatory compliance. This paper introduced a cryptographic passkey authentication framework tailored for healthcare identity and access management (IAM), explored integration strategies for securing electronic health records (EHRs), patient portals, and medical devices, and addressed key challenges such as identity recovery, compliance adherence, and insider threat mitigation. By leveraging passkeys, healthcare organizations can achieve a more secure, efficient, and user-friendly authentication ecosystem, reinforcing trust and safeguarding sensitive medical data.

REFERENCES

[1] Verizon, "2023 Data Breach Investigations Report," Verizon Enterprise, 2023. Available: https://www.verizon.com/business/resources/reports/dbir/.

[2] National Institute of Standards and Technology (NIST), "Digital Identity Guidelines: Authentication and Lifecycle Management," NIST Special Publication 800-63B, 2020. DOI: 10.6028/NIST.SP.800-63b.

[3] U.S. Department of Health & Human Services, "HIPAA Security Rule Standards for Protection of Electronic Protected Health Information," 45 CFR Part 164, 2013. Available: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

[4] FIDO Alliance, "Passkeys: Next-Generation Passwordless Authentication," FIDO Technical Report, 2022. Available: https://fidoalliance.org/specifications/.

[5] A. Narayanan, J. Bonneau, and E. Felten, "The Challenges of Password-Based Authentication in the Digital Age," *IEEE Security & Privacy*, vol. 12, no. 3, pp. 38–45, May–June 2014. DOI: 10.1109/MSP.2014.49.

[6] C. Evans, R. Sleevi, and A. M. Doty, "An Overview of WebAuthn and FIDO2: Standards for Secure and Passwordless Authentication," *ACM Transactions on Privacy and Security (TOPS)*, vol. 24, no. 2, pp. 1–22, 2021. DOI: 10.1145/3469854.

[7] Y. Zou, X. Wang, and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016. DOI: 10.1109/JPROC.2016.2558521.

[8] A. Bhargav-Spantzel, A. Squicciarini, and E. Bertino, "Biometric-Based Secure Authentication in Cloud Computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 2, pp. 167–180, Mar.–Apr. 2012. DOI: 10.1109/TDSC.2012.25.

[9] National Institute of Standards and Technology (NIST), "Post-Quantum Cryptography Standardization," 2022. Available: https://csrc.nist.gov/projects/post-quantum-cryptography.

[10] A. Ng, "Deep learning in cybersecurity: AI-driven risk assessment," Journal of Cybersecurity Research, vol. 45, no. 2, pp. 78–89, 2021. DOI: 10.1234/jcsr.2021.045078.

[11] Sovrin Foundation, "Self-Sovereign Identity & Decentralized Authentication," 2021. Available: https://sovrin.org.

[12] N. Kshetri, "Blockchain and identity management: Security, privacy, and efficiency," IEEE Computer, vol. 51, no. 12, pp. 108-111, Dec. 2018. DOI: 10.1109/MC.2018.2880027