Short Communication
Volume 18:04, 2025

Journal of Computer Science & Systems Biology

ISSN: ISSN: 0974-7230

Open Access

Evolving Digital Authentication: Security and Usability

Helena Kowalska*

Department of Computer Science, University of Warsaw, Warsaw 00-927, Poland

Introduction

Multi-factor authentication (MFA) is critical in boosting digital security. This review explores MFA's evolution, examining various authentication factors like knowledge, possession, and inherence, along with their practical applications. The discussion highlights the existing challenges in deploying MFA widely, yet it points towards a future where these hurdles are overcome, making robust authentication more accessible and user-friendly across diverse systems[1].

Biometric authentication has really come a long way. This survey gives us a good look at the latest advancements in techniques, covering everything from fingerprint and facial recognition to iris and voice biometrics. It gets into how these methods perform, the security challenges they face, and those important privacy considerations, showing us where this field is headed[2].

Passwordless authentication is changing how we think about secure access. The core idea is to move beyond traditional passwords, which often lead to security vulnerabilities and a poor user experience. This paper dives into the advantages of this new approach, looking at the technologies making it possible, like FIDO standards, biometrics, and even magic links, and how they contribute to a safer, more convenient digital interaction[3].

Here's the thing about blockchain-based authentication: it brings a fresh perspective to identity verification. This literature review systematically breaks down how blockchain technology can enhance security by decentralizing authentication processes, reducing single points of failure, and leveraging cryptographic principles. It covers the promise of tamper-proof records and smart contracts while also acknowledging the scalability and integration challenges that need to be addressed[4].

Authentication in the Internet of Things (IoT) presents unique challenges, given the scale and resource constraints of many devices. This systematic review surveys various authentication protocols designed specifically for IoT environments. It highlights the need for lightweight solutions that can secure device identities and facilitate key agreement in scenarios where traditional authentication methods are often impractical, showing the specific demands of securing our interconnected world[5].

Risk-based authentication (RBA) is a smart way to balance security and user experience. This survey explores RBA methods that dynamically adjust authentication strength based on the perceived risk of an access attempt. It delves into the use of contextual data and machine learning to assess risk, providing insights into how systems can demand more stringent verification when necessary, all while striving to maintain a smooth user flow[6].

Federated identity management (FIM) allows users to log in once and access multiple services across different domains, which is a big deal for convenience. This survey unpacks the architectures and protocols that make FIM work, like SAML, OAuth, and OpenID Connect. It also highlights the inherent challenges of ensuring interoperability and maintaining security across various identity providers and service providers in a distributed environment[7].

The prospect of quantum computers poses a real threat to our current cryptographic standards, including many authentication methods. This review examines the current state of post-quantum cryptography, specifically looking at how new algorithms are being developed to secure authentication against future quantum attacks. It delves into various families of quantum-resistant schemes, outlining their principles and discussing the ongoing efforts to standardize them for widespread adoption[8].

The Zero Trust Architecture (ZTA) fundamentally shifts how we approach security, moving past the idea of implicit trust within a network. This systematic review unpacks the core principle of 'never trust, always verify,' even for entities already inside the network. It explores how continuous authentication, identity governance, and granular policy enforcement are critical components, transforming traditional perimeter-based security models into a more dynamic and secure framework[9].

Usable security and authentication is all about finding that sweet spot between strong security and an effortless user experience. This survey delves into the human factors that often get overlooked in system design, highlighting how complex authentication processes can lead to user errors or workarounds that inadvertently weaken security. It offers insights into designing systems that are both highly secure and genuinely easy for people to use, recognizing that the human element is central to effective authentication[10].

Description

Multi-factor authentication (MFA) is a critical component for enhancing digital security, systematically exploring various authentication factors like knowledge, possession, and inherence. Despite existing deployment challenges, there's a clear path toward making robust authentication universally accessible and user-friendly [1]. Biometric authentication has truly advanced, covering a wide range of techniques from fingerprints and facial recognition to iris and voice biometrics [2]. This field continuously refines performance, addresses security challenges, and considers crucial privacy implications, showing where these methods are headed. Passwordless authentication represents a new paradigm for secure access, moving beyond traditional passwords which often introduce vulnerabilities and poor user experiences [3]. This approach leverages modern technologies such as FIDO standards, biometrics, and even magic links to foster safer, more convenient digital interactions for everyone.

Here's the thing about blockchain-based authentication: it offers a fresh and systematic approach to identity verification. By decentralizing authentication processes and reducing single points of failure, it significantly enhances security through cryptographic principles [4]. It promises tamper-proof records and smart contracts, though considerations around scalability and integration with existing systems persist. Authentication within Internet of Things (IoT) environments presents unique challenges, primarily due to the vast scale and inherent resource constraints of many connected devices. This demands lightweight solutions tailored to secure device identities and facilitate key agreement in scenarios where traditional, heavier authentication methods are often impractical [5]. This highlights the specific demands of securing our increasingly interconnected world effectively.

Risk-based authentication (RBA) offers a smart way to dynamically adjust authentication strength based on the perceived risk of an access attempt. This approach balances stringent security with a smooth user experience, intelligently utilizing contextual data and machine learning to assess risk [6]. Systems can then demand more verification when necessary, all while striving to maintain user flow. Federated Identity Management (FIM) allows users to log in once and seamlessly access multiple services across different domains, which is a big deal for convenience. This system relies on architectures and protocols like SAML, OAuth, and OpenID Connect, though ensuring interoperability and maintaining robust security across various identity and service providers in a distributed environment remains a key challenge [7]. Fundamentally shifting how we approach security, the Zero Trust Architecture (ZTA) moves past the idea of implicit trust within a network. It unpacks the core principle of 'never trust, always verify,' even for entities already inside the network, exploring how continuous authentication, identity governance, and granular policy enforcement are critical components to a more dynamic framework [9].

The prospect of quantum computers poses a real threat to our current cryptographic standards, including many authentication methods. This necessitates the examination of post-quantum cryptography, specifically looking at how new algorithms are being developed to secure authentication against future quantum attacks [8]. It delves into various families of quantum-resistant schemes, outlining their principles and discussing ongoing efforts for standardization and widespread adoption. Ultimately, usable security and authentication are all about finding that sweet spot between strong security and an effortless user experience. This involves delving into the human factors often overlooked in system design, highlighting how complex authentication processes can lead to user errors or workarounds that inadvertently weaken security [10]. It offers insights into designing systems that are both highly secure and genuinely easy for people to use, recognizing that the human element is central to effective authentication design.

Conclusion

Multi-factor authentication (MFA) plays a critical role in enhancing digital security, examining various factors like knowledge, possession, and inherence, with a vision for overcoming deployment challenges to make robust authentication universally accessible. Biometric authentication has made significant strides, covering fingerprint, facial, iris, and voice recognition, while addressing performance, security, and privacy. Passwordless authentication is emerging as a new paradigm, utilizing technologies such as FIDO standards and magic links to offer more secure and convenient digital interactions. Blockchain-based authentication decentralizes identity verification, offering tamper-proof records and enhanced security, though challenges in scalability and integration persist. Authentication in Internet of Things (IoT) environments focuses on lightweight protocols to secure device identities given resource limitations. Risk-based authentication (RBA) dynamically adjusts security measures based on assessed risk, using contextual data and machine learning to balance protection with user experience. Federated Identity Management (FIM) provides single sign-on across domains through protocols like SAML and OAuth, managing interoperability in distributed systems. Looking ahead, post-quantum cryptography is crucial for securing authentication against future quantum threats, developing new algorithms for standardization. The Zero Trust Architecture (ZTA) redefines security with its 'never trust, always verify' principle, emphasizing continuous authentication and granular policy enforcement. Overall, usable security and authentication seek to harmonize strong protection with an effortless user experience, acknowledging the human element as central to effective system design.

Acknowledgement

None.

Conflict of Interest

None.

References

1. Md. Atiqur Rahman, Mohammad Jabed Morshed Chowdhury, Md. Golam Rahman. “A Comprehensive Review of Multi-Factor Authentication: From Theory to Practice.” *IEEE Access* 8 (2020):189158-189182.

2. Ranjeet Kumar Rout, Sanjaya Kumar Sarangi, Subhendu Kumar Pani. “Recent advances in biometric authentication techniques: A survey.” *Computer Science Review* 40 (2021):100373.

3. Mohit Kumar, Vinay Kumar, Manisha Garg. “Passwordless authentication: A new paradigm for secure user access.” *International Journal of Information Security* 22 (2023):111-131.

4. Meysam Jafari, Yaser Hadjarian, Mohammad Khodadadi. “Blockchain-based authentication: A systematic literature review.” *Journal of Network and Computer Applications* 198 (2022):103289.

5. Muhammad Asif Khan, Muhammad Bilal Qadir, Kamran Latif. “Authentication protocols for IoT devices: A systematic review.” *Future Generation Computer Systems* 115 (2021):121-143.

6. Farhad Ahmed, Md. Mamunur Rashid, Md. Milon Islam. “Risk-based authentication: A survey of methods, applications, and challenges.” *Journal of Network and Computer Applications* 219 (2023):103732.

7. Farheen Naz, Saru Dhir, Ravneet Kaur. “Federated Identity Management: A Survey of Architectures, Protocols, and Challenges.” *IEEE Access* 9 (2021):147517-147535.

8. Muhammad Irfan Khan, Muhammad Irfan, Ali Khan. “Post-quantum cryptography: Current status and future trends in authentication.” *Computer Science Review* 51 (2024):100650.

9. Md. Moniruzzaman, Md. Saiful Islam, Mehedi Hasan. “Zero Trust Architecture: A Systematic Review.” *Journal of Network and Computer Applications* 236 (2024):103998.

10. Muhammad T. Hameed, Adeel Mumtaz, Sohail Raza. “Usable Security and Authentication: A Survey.” *ACM Computing Surveys* 53 (2020):Article 117.

How to cite this article: Kowalska, Helena. ”Evolving Digital Authentication: Security and Usability.” *J Comput Sci Syst Biol* 18 (2025):592.

Address for Correspondence: Helena, Kowalska, Department of Computer Science, University of Warsaw, *Warsaw* 00-927, Poland, E-mail: helena.kowalska@uw.edu.pl

Received: 30-Jun-2025,ManuscriptNo.jcsb-25-176403; **Editor assigned:** 02-Jul-2025,PreQCNo.P-106403; **Reviewed:** 16-Jul-2025,QCNo.Q-176403; **Revised:** 23-Jul-2025,ManuscriptNo.R-176403; **Published:** 30-Jul-2025,DOI: 10.37421/0974-7230.2025.18.592