Durojaye Emmanuel Olatunji, 2026, 14:4
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Comparative Analysis of Password-based, Multi-factor, and Biometric Authentication Methods and their Effectiveness in Reducing Unauthorized Access

Durojaye Emmanuel Olatunji[1], Akinola Daniel Adeoye[2], Ajayi Titus Ileriayo[3], Adebayo Suliat Precious[4], Adewale Joseph Adebiyi[5]

[1'2,3,4,5]Department of Software and Web Development
Ogun State Institute of Technology (OGITECH), Igbesa Ogun state, Nigeria

Abstract- Software security has become increasingly important as organizations and individuals continue to depend on digital systems for communication, financial transactions, healthcare, education, and other critical services. One of the primary mechanisms used to protect these systems from unauthorized access is user authentication. Traditional password-based authentication remains the most widely adopted authentication method because of its simplicity and low implementation cost. However, the growing sophistication of cyberattacks, including phishing, brute-force attacks, credential stuffing, and password reuse, has exposed significant weaknesses in password-only authentication systems, prompting the development of more advanced techniques such as multi-factor authentication and biometric authentication. [1,2] This study assesses password authentication techniques for enhancing software security through a comparative analysis of password-based authentication, multi-factor authentication, and biometric authentication. A qualitative comparative research design was adopted using secondary data obtained from textbooks, peer-reviewed journal articles, conference proceedings, and international standards, with techniques evaluated on security effectiveness, usability, implementation cost, reliability, and resistance to cyberattacks. [3,5] Findings indicate that although password-based authentication remains essential because of its widespread acceptance, combining it with additional authentication factors significantly improves software security and reduces the risk of unauthorized access. The study concludes that organizations should adopt multi-layered authentication mechanisms to achieve stronger protection for modern software applications.

Keywords— Software Security, Password Authentication, Multi-Factor Authentication, Biometric Authentication, Cybersecurity.

I. INTRODUCTION

The rapid advancement of information and communication technology has transformed the way organizations, governments, and individuals store, process, and exchange information. Software applications are now widely used in banking, healthcare, education, electronic commerce, and public administration, making the protection of digital information a major concern. As dependence on software systems continues to increase, cybercriminals have developed more sophisticated techniques for exploiting vulnerabilities in authentication systems to gain unauthorized access to sensitive information. [1,2]

Authentication is a fundamental component of software security because it verifies the identity of users before granting access to protected resources, helping maintain the confidentiality, integrity, and availability of information. [1] Among the various authentication techniques, password-based

authentication remains the most commonly implemented because it is simple, inexpensive, and easy to deploy across different computing environments. Despite these advantages, password-only authentication has become increasingly vulnerable to attacks such as phishing, dictionary attacks, brute-force attacks, credential stuffing, and password reuse, resulting in frequent security breaches and unauthorized system access. [2,3]

To address the limitations associated with traditional passwords, software developers and security researchers have introduced stronger authentication mechanisms, including multi-factor authentication and biometric authentication. Multi-factor authentication enhances security by requiring users to provide multiple forms of identity verification, while biometric authentication relies on unique physiological or behavioral characteristics such as fingerprints, facial recognition, iris patterns, and voice recognition to establish user identity. [4,5] These techniques have significantly improved software security, although each presents its own advantages and implementation challenges.

Several studies have demonstrated that combining multiple authentication factors provides greater protection than relying solely on passwords. Nevertheless, organizations continue to face challenges in selecting authentication methods that provide an appropriate balance between security, usability, implementation cost, and user convenience, creating a growing need to evaluate the effectiveness of existing authentication techniques. [3,5]

This study therefore assesses password authentication techniques for enhancing software security through a comparative analysis of password-based authentication, multi-factor authentication, and biometric authentication, with findings intended to provide useful insights for software developers, organizations, researchers, and policymakers in reducing unauthorized access.

This paper is structured as follows: Section 2 reviews related literature. Section 3 describes the methodology. Section 4 presents results and discussion. Section 5 concludes with key recommendations.

II. RELATED STUDIES / LITERATURE REVIEW

The increasing dependence on digital technologies has resulted in significant research efforts aimed at improving authentication mechanisms for protecting software systems against unauthorized access. Authentication remains one of the most important security controls because it serves as the first line of defense against cyber threats. Researchers have proposed and evaluated several authentication techniques, including password-based authentication, multi-factor authentication, and biometric authentication, each offering different levels of security, usability, and implementation complexity. [2,3]

1. Authentication in Software Security

Authentication is the process of verifying the identity of a user, device, or system before access to protected resources is granted, and it plays a critical role in ensuring confidentiality, integrity, and availability of information within software applications. Authentication mechanisms prevent unauthorized users from accessing sensitive resources and reduce the likelihood of security breaches, and should resist modern cyberattacks such as phishing, credential theft, replay attacks, and social engineering. [1,2]

Recent studies emphasize that authentication systems must achieve an appropriate balance between security and usability, since highly secure mechanisms may become inconvenient for users, while highly convenient mechanisms may expose systems to additional risk. Researchers have proposed evaluation criteria that consider security effectiveness, usability, privacy, reliability, deployment cost, and resistance to various attack models when assessing authentication systems.

2. Password-Based Authentication

Password-based authentication remains the most widely deployed authentication technique because of its simplicity, low implementation cost, and

compatibility with virtually every software platform, verifying users against stored credentials such as a username and password. [1]

Despite widespread adoption, numerous researchers have identified significant weaknesses associated with password-based authentication. Weak passwords, password reuse, phishing attacks, brute-force attacks, dictionary attacks, credential stuffing, and keylogging continue to compromise password-only systems, with attackers frequently exploiting human behavior rather than technical vulnerabilities. As a result, password compromise continues to be one of the leading causes of unauthorized access in modern information systems. [4]

To reduce these risks, researchers recommend enforcing strong password policies, implementing password managers, limiting login attempts, applying account lockout mechanisms, and integrating additional authentication factors rather than relying exclusively on passwords. [3]

3. Multi-Factor Authentication

Multi-factor authentication (MFA) enhances software security by requiring users to present two or more independent authentication factors before access is granted. These factors generally include something the user knows (password or PIN), something the user possesses (security token, mobile device, or smart card), and something the user is (biometric characteristic).

Recent surveys indicate that MFA significantly reduces the probability of successful unauthorized access even when passwords have been compromised, with modern implementations combining one-time passwords, authenticator applications, hardware security keys, and biometric verification. Nevertheless, some traditional MFA methods, particularly SMS-based verification, remain susceptible to sophisticated phishing and social engineering attacks, and current research increasingly recommends phishing-resistant authentication methods based on cryptographic standards and hardware-backed credentials. [7,9]

4. Biometric Authentication

Biometric authentication verifies user identity using unique physiological or behavioral characteristics such as fingerprints, facial recognition, iris recognition, voice recognition, and palm vein patterns. Unlike passwords, biometric characteristics cannot easily be forgotten, shared, or guessed, making them attractive for modern authentication systems.

Research reviewing recent developments in biometric authentication concludes that biometric systems provide stronger identity verification while improving user convenience, though important challenges remain, including privacy concerns, spoofing attacks, template protection, biometric data leakage, and implementation costs, requiring continuous improvements in biometric security technologies and privacy-preserving authentication protocols. [5,6]

5. Comparative Review of Previous Studies

Previous research consistently demonstrates that no single authentication technique provides complete protection against every security threat. Password-based authentication remains suitable for many low-risk applications because of its simplicity and affordability; however, studies consistently report that password-only authentication provides weaker protection against modern cyberattacks than methods that combine multiple verification factors.
Multi-factor authentication significantly improves security by introducing additional verification layers, reducing the effectiveness of credential theft and password compromise. Similarly, biometric authentication offers high levels of identity assurance but introduces concerns relating to privacy, cost, and secure storage of biometric templates. Current research therefore supports layered authentication approaches that combine passwords with additional factors to improve overall software security while maintaining acceptable usability.

6. Research Gap

Although numerous studies have investigated password-based authentication, multi-factor authentication, and biometric authentication

individually, comparatively fewer studies provide a comprehensive evaluation of these techniques using common assessment criteria such as security effectiveness, usability, implementation cost, reliability, and resistance to cyberattacks. Furthermore, the rapid evolution of phishing-resistant authentication technologies and passwordless authentication frameworks has created a need for updated comparative assessments that assist software developers and organizations in selecting appropriate authentication mechanisms. This study addresses this gap by providing a comparative assessment of the three authentication techniques within the context of enhancing software security.

III. METHODOLOGY

This study adopted a qualitative comparative research design to assess password authentication techniques for enhancing software security, synthesizing findings from existing academic literature rather than conducting experimental testing or user surveys. [1,2]

1. Research Design

A qualitative comparative research design was employed, considered appropriate because it enabled the systematic comparison of password-based authentication, multi-factor authentication, and biometric authentication using established evaluation criteria reported in previous scholarly studies. This approach identifies the strengths, weaknesses, and practical applications of each authentication technique. [1,2]

2. Data Collection

The study relied exclusively on secondary data obtained from reputable academic sources, including peer-reviewed journal articles, conference proceedings, textbooks, international security standards, and technical reports published by recognized organizations. Selected literature focused on authentication mechanisms, software security, cybersecurity threats, identity management, and modern access control systems, with priority given to recent publications to ensure findings reflected current developments in authentication technologies and emerging cyber threats. [3,4]

3. Analytical Framework

Authentication techniques were assessed using five major comparison criteria identified from previous studies: security effectiveness, usability, implementation cost, reliability, and resistance to cyberattacks. Security effectiveness measured the ability of an authentication method to prevent unauthorized access; usability evaluated the convenience and ease of use for legitimate users; implementation cost considered the financial and technical resources required for deployment; reliability measured consistency of performance under normal operating conditions; and resistance to cyberattacks examined the ability of each technique to withstand attacks such as phishing, brute-force attacks, credential stuffing, replay attacks, and spoofing. [2,5,6]

The comparative analysis involved reviewing the findings reported by different researchers and identifying common patterns regarding the performance of the three authentication techniques, allowing objective conclusions to be drawn regarding their effectiveness in enhancing software security. The findings are presented in tabular form and discussed in detail in the subsequent section of this paper. This methodology provides a structured framework for evaluating authentication mechanisms using evidence obtained from existing scholarly literature, ensuring that findings are supported by credible academic sources while providing practical recommendations for selecting appropriate authentication techniques in modern software applications.

IV. RESULTS AND DISCUSSION

This section presents the findings obtained from the comparative assessment of password-based authentication, multi-factor authentication, and biometric authentication, evaluated using five key criteria: security effectiveness, usability, implementation cost, reliability, and resistance to cyberattacks. [1,2]

1. Comparative Analysis of Authentication Techniques

The comparative assessment indicates that password-based authentication remains the most widely deployed authentication mechanism because of its simplicity, low implementation cost, and ease of deployment, supported by virtually all software platforms with minimal hardware resources. However, password-only authentication provides the lowest level of protection against modern cyber threats: weak passwords, password reuse, phishing attacks, brute-force attacks, credential stuffing, and keylogging continue to compromise password-based systems, making them increasingly inadequate for protecting sensitive information. [2,4] Multi-factor authentication significantly improves software security by requiring users to provide multiple independent authentication factors before access is granted, ensuring that even if an attacker obtains a user's password, additional verification factors are still required. Consequently, MFA has become one of the most recommended mechanisms for protecting financial systems, cloud services, enterprise applications, and online platforms. Although implementation introduces additional steps that may slightly reduce user convenience, the security benefits considerably outweigh these limitations. [3,6]

Biometric authentication provides a different approach by verifying users through unique physiological or behavioral characteristics, including fingerprints, facial recognition, iris recognition, and voice recognition. The uniqueness of biometric characteristics makes impersonation significantly more difficult than password guessing, and biometric authentication improves usability because users no longer need to remember complex passwords. Nevertheless, concerns regarding biometric privacy, template protection, implementation cost, and spoofing attacks continue to present important research challenges. [5]

2. Comparative Analysis Table

Table 1 presents the comparative evaluation of the three authentication techniques using the selected assessment criteria.

- Password-Based Authentication: simple; low cost; weak security; easy to attack.
- Multi-Factor Authentication: strong security; multiple verification (OTP, app, SMS); higher protection.
- Biometric Authentication: unique identity; hard to replicate; privacy concerns; expensive systems.

The comparative analysis demonstrates that password-based authentication performs well in terms of usability and affordability but performs poorly when evaluated against modern cyber threats. Multi-factor authentication consistently achieves higher security ratings because multiple verification factors significantly reduce the probability of unauthorized access. Biometric authentication also provides strong authentication capabilities; however, its deployment often requires specialized hardware and secure biometric data management, increasing implementation costs. [5,6]

3. Authentication Process Flow

The general authentication process used by modern software systems begins when a user attempts to access a software application. The system requests authentication credentials, which may include a password, one-time verification code, or biometric information. The supplied credentials are validated against stored authentication records; if verification is successful, access is granted, otherwise access is denied and appropriate security measures such as account lockout or additional verification may be initiated (User → Authentication Method → Credential Verification → Access Granted or Denied).

4. Discussion of Findings

The findings of this study demonstrate that no single authentication technique completely satisfies every security and usability requirement. Password-based authentication continues to dominate because of its simplicity and widespread adoption, yet it remains the authentication method most frequently compromised by cybercriminals, exposing organizations relying solely on passwords to increased cybersecurity risk. [2,4]

The study further confirms that multi-factor authentication provides the most balanced solution by combining strong security with acceptable usability, explaining why many technology companies, financial institutions, educational platforms, and government agencies increasingly require MFA for user accounts. [3,6]

Biometric authentication also offers considerable advantages, particularly in mobile devices, healthcare systems, and high-security facilities where accurate identity verification is essential. However, concerns regarding biometric privacy, data protection, and implementation costs continue to influence its adoption across different sectors. [5]

Overall, the comparative analysis indicates that integrating password-based authentication with multi-factor authentication provides significantly greater protection than relying on passwords alone. For highly sensitive applications, combining passwords, multi-factor authentication, and biometric authentication offers the strongest level of software security currently available.

V. CONCLUSION

Software security has become increasingly important due to the rapid growth of digital technologies and the increasing frequency of cyberattacks targeting information systems. Authentication remains one of the most fundamental security mechanisms for preventing unauthorized access and protecting sensitive digital resources. This study assessed password authentication techniques for enhancing software security through a comparative evaluation of password-based authentication, multi-factor authentication, and biometric authentication.

The findings revealed that password-based authentication continues to be the most widely implemented authentication technique because of its simplicity, affordability, and ease of deployment. However, it is also the most vulnerable authentication method due to weaknesses such as password reuse, phishing attacks, brute-force attacks, credential stuffing, and other forms of credential compromise, meaning that relying solely on password-based authentication is no longer sufficient for protecting modern software applications against evolving cyber threats. [2,4]

The study further established that multi-factor authentication significantly strengthens software security by introducing additional layers of identity verification, so that even when passwords are compromised, unauthorized users cannot gain access without satisfying additional requirements. Similarly, biometric authentication provides strong identity verification through unique physiological and behavioral characteristics, improving both security and user convenience, although concerns relating to privacy, implementation cost, biometric template protection, and spoofing attacks continue to influence its widespread adoption. [5,6]

Key recommendations arising from this research include: adopting layered authentication strategies that combine password-based authentication with multi-factor authentication and, where appropriate, biometric authentication; enforcing strong password policies and account lockout mechanisms; and prioritizing phishing-resistant, hardware-backed authentication methods for sensitive systems. Such integrated approaches provide stronger protection against unauthorized access while maintaining acceptable usability, reliability, and operational efficiency.

No single authentication technique completely satisfies every security requirement. Future studies may extend this work by experimentally evaluating emerging passwordless authentication technologies, behavioral biometrics, artificial intelligence-based authentication systems, and decentralized identity management frameworks, which represent promising directions for improving software security as cyber threats continue to evolve.

REFERENCES

1. W. Stallings, Cryptography and Network Security: Principles and Practice, 8th ed. Harlow, United Kingdom: Pearson, 2021.

2. R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd ed. Indianapolis, IN, USA: Wiley, 2020.
3. P. A. Grassi, M. E. Garcia, and J. L. Fenton, Digital Identity Guidelines: Authentication and Lifecycle Management (NIST Special Publication 800-63B). Gaithersburg, MD, USA: National Institute of Standards and Technology, 2020.
4. X. Wang, Z. Yan, R. Zhang, and P. Zhang, "Attacks and Defenses in User Authentication Systems: A Survey," Journal of Network and Computer Applications, vol. 188, 2021.
5. A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4–20, Jan. 2004.
6. R. Zhang and Z. Yan, "A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification," IEEE Access, vol. 7, pp. 5994–6009, 2019.
7. A. H. Y. Mohammed, R. A. Dziyauddin, and L. A. Latiff, "Current Multi-Factor Authentication: Approaches, Requirements, Attacks and Challenges," International Journal of Advanced Computer Science and Applications, vol. 14, no. 1, pp. 174–188, 2023.
8. S. Furnell and P. Dowland, "A Review of Contemporary Authentication Technologies and Their Usability," Computers & Security, vol. 118, 2022.
9. M. Aloul, S. Zahidi, and W. El-Hajj, "Two Factor Authentication Using Mobile Phones," Proceedings of the IEEE/ACS International Conference on Computer Systems and Applications, pp. 641–644, 2009.
10. FIDO Alliance, FIDO2: Moving the World Beyond Passwords, FIDO Alliance Technical Overview, 2023.