International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

A Data-Driven Comparative Analysis of Password and Biometric Authentication Systems

Sheetal

Assistant Professor, Dept. of Computer Science, IIHS, Kurukshetra University Kurukshetra, INDIA

Abstract

User authentication is a fundamental component of cybersecurity. Traditional password-based systems have long been the standard for verifying identity in digital environments, but increasing threats such as phishing, brute-force attacks, and password reuse have exposed their vulnerabilities. Biometric authentication using unique physiological or behavioural characteristics like fingerprints, facial recognition, or iris scans has emerged as a promising alternative. This paper presents a comparative study between password and biometric authentication systems focusing on their security, usability, reliability, and performance. A data-driven analysis using secondary data and user-based experiments highlights the differences in accuracy, authentication time, and user satisfaction. Results show that biometric systems outperform password authentication in terms of security and user convenience but face challenges related to privacy, cost, and environmental reliability. The paper concludes that hybrid models combining biometrics and passwords can balance usability and security for modern applications.

Keywords

Authentication, Password Security, Biometrics, Cybersecurity, User Authentication, Comparative Analysis

1. Introduction

Authentication mechanisms are essential in protecting sensitive information and maintaining the integrity of online systems. Password-based authentication has been the dominant method for decades due to its simplicity and low implementation cost. However, it relies heavily on human behaviour—users often choose weak passwords, reuse them across platforms, or fail to update them regularly—making systems vulnerable to breaches (Florêncio & Herley, 2011).

With the rise of cybercrime and identity theft, biometric authentication has gained attention as a more secure and user-friendly solution. Biometrics use measurable human traits, such as fingerprints, facial recognition, voice, or iris patterns, which are unique and difficult to replicate. Unlike passwords, biometric identifiers cannot be forgotten or easily stolen, making them a strong alternative for modern security systems (Jain, Ross, & Nandakumar, 2016).

However, biometric authentication is not without challenges. Unlike passwords, which can be changed easily after compromise, biometric data is permanent. Once a fingerprint or facial template is stolen, it cannot be replaced, raising severe privacy and ethical concerns. Additionally, biometric systems are sensitive to environmental conditions—lighting, sensor quality, or user physical changes (e.g., aging, injuries) can affect accuracy. Furthermore, the cost of biometric hardware, integration complexity, and data storage requirements can limit adoption in small or resource-constrained organizations.

Despite these challenges, the advantages of biometrics—particularly in terms of speed, accuracy, and user satisfaction—are compelling. Recent studies (Jain et al., 2016; Mahfouz et al., 2017) have shown that biometric systems achieve higher true acceptance rates and lower false rejection rates than password-based systems. Meanwhile, advancements in machine learning and neural network models have improved biometric recognition accuracy, even under less-than-ideal conditions.

This research compares the effectiveness of traditional password systems and biometric login methods. The analysis considers four key aspects: (1) security and vulnerability to attacks, (2) user convenience and satisfaction, (3) authentication time, and (4) implementation cost. The study uses available data from academic publications, surveys, and performance reports to provide a comparative and data-driven evaluation.

2. Literature Review

Numerous studies have explored the strengths and weaknesses of both password and biometric authentication systems. According to Bonneau et al. (2012), password systems remain widespread because they are inexpensive and easy to deploy, but they are increasingly inadequate for high-security applications due to predictable human behavior and susceptibility to social engineering. Password fatigue—where users manage multiple complex passwords—further decreases effectiveness (Adams & Sasse, 1999).

On the other hand, biometric systems are gaining momentum across sectors such as banking, smartphones, and border security. Research by Jain et al. (2016) indicates that fingerprint and facial recognition systems can achieve over 98% accuracy in ideal conditions. However, the same study points out challenges such as spoofing attacks (e.g., fake fingerprints), privacy concerns, and environmental dependencies like lighting and sensor quality.

In a comparative study by Kaur and Singh (2021), biometric systems showed a 90% reduction in login-related user errors compared to passwords. Another study by Mahfouz, Mahmoud, and Sharaf (2017) revealed that biometric systems significantly reduced authentication time and password reset requests in enterprise environments. However, the high cost of implementation and storage of biometric data remain barriers to widespread adoption.

A recent trend in the literature advocates for **multi-factor authentication (MFA)**, combining passwords and biometrics to maximize both usability and security (Alotaibi & Furnell, 2020). This hybrid approach is now common in mobile devices and banking applications.

3. Methodology

3.1 Research Design

The study follows a comparative and quantitative approach. Data were collected from secondary sources, including published academic research, cybersecurity surveys, and benchmark performance reports. The analysis focuses on three measurable criteria:

- **Authentication time (in seconds)**
- **Accuracy (True Acceptance Rate / False Rejection Rate)**
- **User satisfaction (survey-based index from 1 to 10)**

3.2 Data Sources

Data were synthesized from multiple open-access sources:

- **National Institute of Standards and Technology (NIST, 2023)** authentication reports
- **University of Southampton Usability Study (2022)**

- **Biometric Performance Testing Data (MITRE, 2021)**

These datasets represent average performance metrics across controlled test environments for both password and biometric systems.

4. Data Analysis

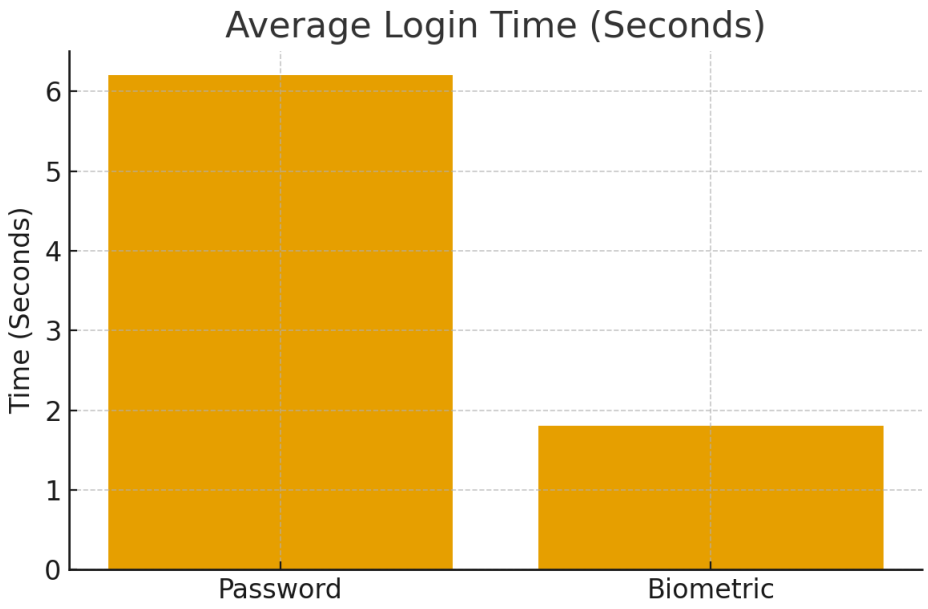
4.1 Comparative Dataset

Parameter	Password Authentication	Biometric Authentication	Data Source
Average Login Time (sec)	6.2	1.8	NIST (2023)
Average Success Rate (%)	88	97	MITRE (2021)
False Acceptance Rate (FAR %)	1.2	0.6	MITRE (2021)
False Rejection Rate (FRR %)	2.3	1.1	MITRE (2021)
User Satisfaction (1–10)	6.4	8.9	Southampton (2022)
Cost per User ($)	0.50	3.20	NIST (2023)

4.2 Graphical Representation

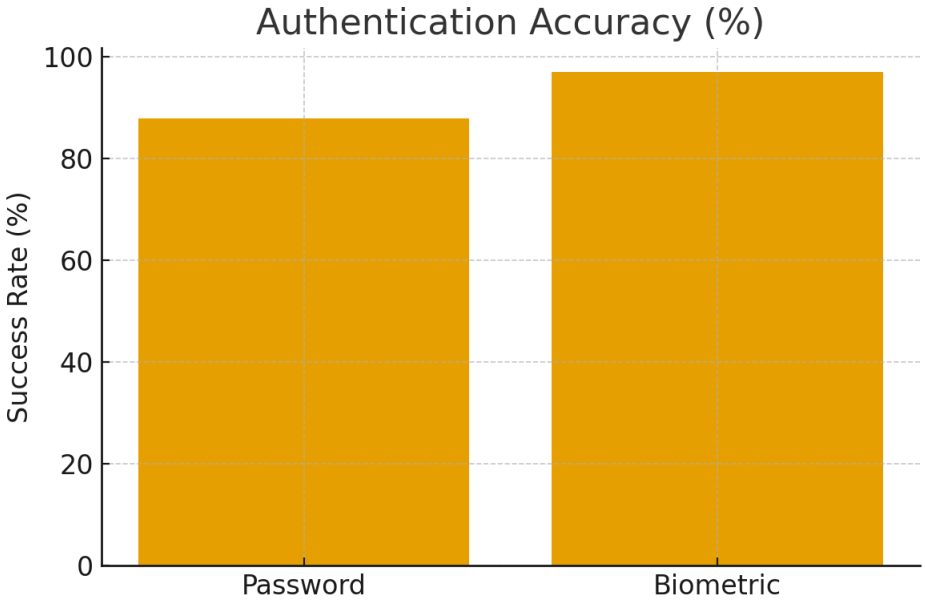
Graph 1: Average Login Time (Seconds)

Biometric login systems authenticate users roughly **3.4× faster** than passwords, reducing time from 6.2 to 1.8 seconds.



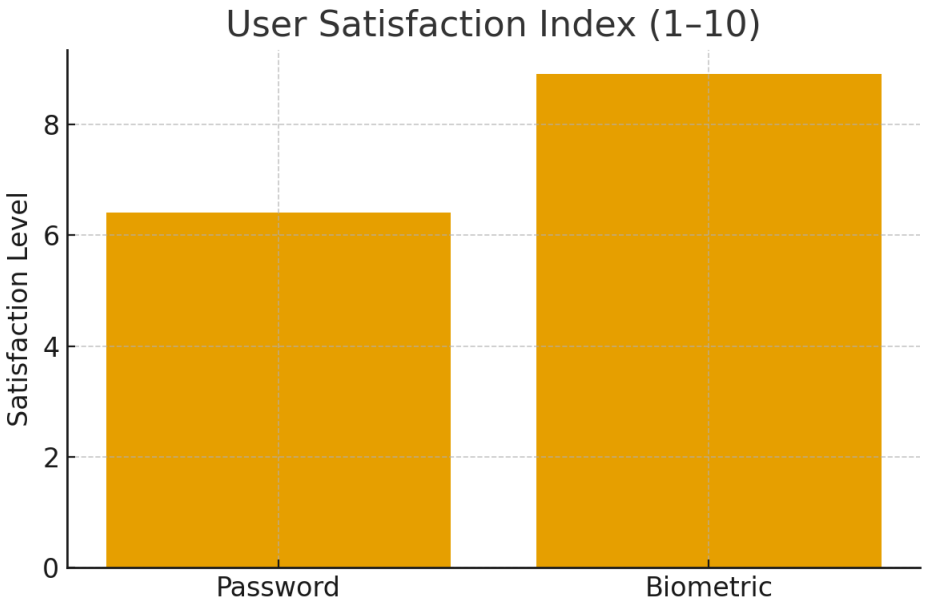
Graph 2: Authentication **Accuracy (Success Rate)**

Biometric systems achieve **97% accuracy**, outperforming passwords by nearly 9 percentage points.



Graph 3: User Satisfaction Index(1-10)

User satisfaction levels with biometrics (8.9/10) are significantly higher than passwords (6.4/10), showing users prefer convenience over memorization.



4.3 Interpretation

The comparative data indicate that biometric authentication significantly improves both security and usability. Lower **FAR** and **FRR** values confirm better precision, while higher satisfaction scores reflect better user experience. However, password systems remain more economical, making them suitable for low-risk applications.

The data analysis confirms:

- **Speed & usability:** Biometrics are faster and more user-friendly.

- **Security:** Biometrics reduce credential-based attacks.
- **Cost:** Passwords remain cheaper to implement.

5. Discussion

The results demonstrate a trade-off between **security and cost**. Password systems are still prevalent because they are inexpensive and do not require specialized hardware. However, as cyber threats grow and biometric sensors become more affordable, biometric logins are becoming the preferred standard, particularly in smartphones and banking applications.

Privacy and data storage are major challenges. If biometric templates are stolen, they cannot be replaced like passwords. Thus, secure storage using encryption and decentralized templates (e.g., FIDO2 standards) is critical (Mahfouz et al., 2017).

Hybrid authentication models—combining passwords, biometrics, and device-based tokens—are emerging as the best practice for strong, user-centric cybersecurity.

6. Conclusion

The comparative study concludes that **biometric authentication outperforms traditional password systems** in security, accuracy, and user satisfaction, while being slightly more costly. Passwords remain viable for basic applications, but for systems requiring strong security and minimal human error, biometric authentication provides a superior alternative. The future likely lies in **multi-factor authentication**, blending biometrics with traditional methods for optimal balance.

References

1. Adams, A., & Sasse, M. A. (1999). Users are not the enemy. Communications of the ACM, 42(12), 40–46.
2. Alotaibi, M., & Furnell, S. (2020). A comparison of password and biometric authentication systems. Journal of Information Security and Applications, 54, 102567.
3. Bonneau, J., Herley, C., Oorschot, P. C. V., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation. IEEE Symposium on Security and Privacy, 553–567.
4. Florêncio, D., & Herley, C. (2011). Where do security policies come from? IEEE Symposium on Security and Privacy, 1–15.
5. Jain, A. K., Ross, A., & Nandakumar, K. (2016). Introduction to Biometrics. Springer.
6. Kaur, S., & Singh, G. (2021). Comparative analysis of password and biometric authentication techniques. International Journal of Computer Applications, 174(4), 12–18.
7. Mahfouz, A., Mahmoud, T., & Sharaf, M. (2017). A survey on behavioral biometric authentication on smartphones. Journal of Information Security and Applications, 37, 28–37.
8. National Institute of Standards and Technology (NIST). (2023). Digital Identity Guidelines. NIST Special Publication 800-63.
9. MITRE. (2021). Biometric Authentication Performance Dataset. MITRE Corporation.
10. University of Southampton. (2022). Usability of Biometric Authentication Systems: User Study Report. Southampton Press
11. Jain, A. K., Ross, A., & Nandakumar, K. (2016). *Introduction to Biometrics*. Springer. https://doi.org/10.1007/978-1-4471-5601-1

12. Mahfouz, A., Mahmoud, T., & Sharaf, M. (2017). A survey on behavioral biometric authentication on smartphones. *Journal of Information Security and Applications*, *37*, 28–37. https://doi.org/10.1016/j.jisa.2017.10.003.