The Evolution of Identity and Access Management: Integrating Biometric and Behavioral Authentication

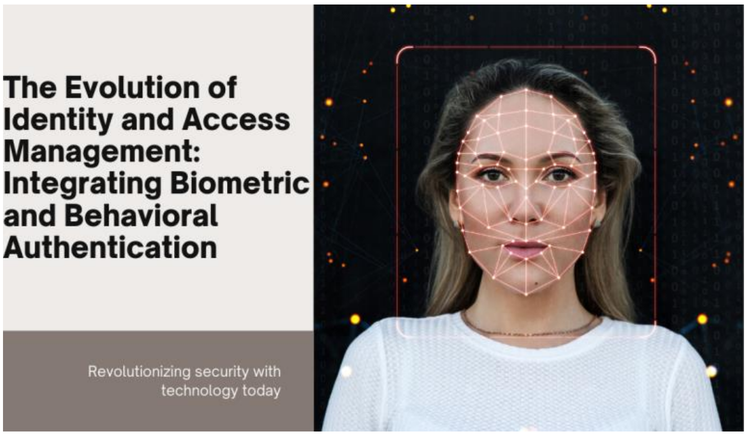
Sharath Chandra Thurupati

MSR Technology Group, USA

Abstract

This article explores the transformative role of biometric and behavioral authentication in the evolving landscape of Identity and Access Management (IAM). As traditional password-based systems increasingly fail to meet the challenges posed by sophisticated cyber threats, these advanced authentication methods offer a promising solution. The article provides a comprehensive overview of physical and behavioral biometrics, examining their integration into multi-factor authentication systems and their capacity for continuous, passive user verification. It delves into the significant security benefits these technologies offer, including enhanced resistance to phishing, social engineering, and insider threats, while also highlighting the improvements in user experience and convenience. The article critically analyzes the challenges and considerations associated with implementing biometric and behavioral authentication, including privacy concerns, data security, accuracy issues, and scalability. Furthermore, it explores future directions and research opportunities in the field, such as advancements in biometric technologies, the application of machine learning and AI in behavioral analysis, and the development of context-aware authentication systems. By synthesizing current research and industry trends, this article provides valuable insights for cybersecurity professionals, IT decision-makers, and researchers interested in the future of secure and user-friendly authentication methods. It underscores the potential of biometric and behavioral authentication to significantly enhance organizational security postures while improving user satisfaction in an increasingly digital world.

Keywords: Biometric Authentication, Behavioral Biometrics, Continuous Authentication, Multi-factor Authentication (MFA), Identity and Access Management (IAM)


The Evolution of Identity and Access Management: Integrating Biometric and Behavioral Authentication
Revolutionizing security with technology today

I. Introduction

The landscape of cybersecurity is rapidly evolving, with traditional password-based systems increasingly proving inadequate in the face of sophisticated threats. As organizations grapple with the challenges of securing digital assets and user identities, biometric and behavioral authentication technologies are emerging as pivotal components in the future of Identity and Access Management (IAM). These advanced methods leverage unique physical characteristics and behavioral patterns to verify user identities, offering a more robust and user-friendly alternative to conventional approaches. The integration of biometrics and behavioral analysis into IAM systems promises to enhance security measures while simultaneously improving the user experience. This shift is particularly crucial as cyber attacks become more sophisticated, with global cybercrime damages projected to reach $10.5 trillion annually by 2025 [1]. By moving beyond the limitations of passwords and embracing these innovative authentication techniques, organizations can significantly strengthen their security posture, mitigate risks associated with credential theft and phishing, and provide a seamless authentication experience for users. This article explores the current state and future potential of biometric and behavioral authentication in IAM, examining their benefits, challenges, and implications for the evolving cybersecurity landscape.

II. Background: The Shift from Passwords to Biometrics

A. Vulnerabilities of password-based systems

Traditional password-based authentication systems have long been the cornerstone of digital security, but their vulnerabilities have become increasingly apparent in recent years. These systems are susceptible to a wide range of attacks, including brute force attempts, dictionary attacks, and social engineering techniques such as phishing. The human factor plays a significant role in these vulnerabilities, as users often choose weak, easily guessable passwords or reuse the same password across multiple accounts. Moreover, the increasing sophistication of cyber attacks has made it easier for malicious actors to crack or bypass password protections, leading to data breaches and unauthorized access to sensitive information.

B. The need for stronger authentication methods

The limitations of password-based systems have created a pressing need for more robust authentication methods. Organizations are seeking solutions that can provide higher levels of security while maintaining user convenience. This demand has driven the development and adoption of multi-factor authentication (MFA) systems, which combine multiple authentication factors to verify a user's identity. However, even MFA systems that rely on knowledge-based factors (like passwords) and possession-based factors (like tokens or smartphones) can still be compromised through sophisticated attack vectors.

C. Introduction to biometric authentication

Biometric authentication has emerged as a promising solution to address the shortcomings of traditional password-based systems. This technology leverages unique physical or behavioral characteristics of individuals to verify their identity, offering a more secure and user-friendly alternative to passwords. Biometric authentication methods can be broadly categorized into two types: physical biometrics, which include fingerprints, facial recognition, and iris scans; and behavioral biometrics, which analyze patterns in user behavior such as typing rhythm, mouse movements, or gait.

Advancements in sensor technologies, machine learning algorithms, and the widespread availability of biometric-capable devices such as smartphones have accelerated the adoption of biometric authentication. These factors have contributed to improving the accuracy, speed, and cost-effectiveness of biometric systems. Research has shown that biometric authentication can significantly enhance security while reducing friction in the user experience. For instance, a study demonstrated that a multi-modal biometric system combining fingerprint and iris recognition achieved an equal error rate of just 0.03%, substantially outperforming traditional authentication methods [2].

As organizations continue to prioritize cybersecurity and seek more effective ways to protect digital assets and user identities, biometric authentication is poised to play an increasingly important role in the future of Identity and Access Management. The transition from passwords to biometrics represents a paradigm shift in how we approach digital security, offering the potential to dramatically reduce the risk of unauthorized access while improving the overall user experience.

III. Types of Biometric Authentication

A. Physical Biometrics

Physical biometrics rely on unique physiological characteristics of individuals for authentication. These methods have gained widespread adoption due to their accuracy and ease of use.

1. Fingerprints: Fingerprint recognition remains one of the most widely used biometric authentication methods. It analyzes the unique patterns of ridges and valleys on a person's fingertips. Modern fingerprint sensors use various technologies, including optical, capacitive, and ultrasonic, to capture high-resolution images of fingerprints. The accuracy and speed of fingerprint recognition have improved significantly, with some systems achieving false acceptance rates as low as 0.01% [3].
2. Facial recognition: This technology analyzes facial features and geometry to identify individuals. Advanced facial recognition systems use 3D mapping and deep learning algorithms to improve accuracy and resist spoofing attempts. The convenience of facial recognition has led to its integration in many smartphones and security systems.
3. Voice recognition: Voice biometrics authenticate users based on the unique characteristics of their voice, including pitch, tone, and speech patterns. This method is particularly useful for remote authentication scenarios, such as phone banking or voice-activated smart home devices.
4. Retinal and iris scans: These methods analyze the unique patterns in the retina or iris of the eye. Iris recognition, in particular, has gained traction due to its high accuracy and the fact that iris patterns remain stable throughout a person's life. Some studies have shown iris recognition systems achieving equal error rates as low as 0.0001% [4].

B. Behavioral Biometrics

Behavioral biometrics focus on identifying individuals based on their unique patterns of behavior. These methods offer the advantage of continuous authentication without requiring explicit user actions.

1. Typing patterns: This method analyzes how a user types, including factors such as typing speed, rhythm, and common errors. It can be used for continuous authentication during computer use.
2. Keystroke dynamics: Similar to typing patterns, keystroke dynamics examine the specific way a user interacts with a keyboard, including the duration of key presses and the time between key presses. This method can provide a unique "fingerprint" of a user's typing behavior.
3. Mouse movements: Mouse dynamics analysis examines patterns in how a user moves and clicks the mouse. This can include factors such as cursor speed, click frequency, and movement patterns.
4. Gait analysis: This emerging behavioral biometric method analyzes an individual's walking pattern. It can be particularly useful for passive authentication in environments with video surveillance or when using mobile devices with built-in accelerometers.

Behavioral biometrics offer the advantage of continuous, passive authentication, potentially detecting unauthorized access even after initial login. For example, a study demonstrated that a multi-modal behavioral biometric system combining keystroke dynamics and mouse movements could achieve an equal error rate of 2.46%, showing promise for real-world applications [5].

The combination of physical and behavioral biometrics in multi-modal systems can provide even stronger authentication, leveraging the strengths of each method to create a more robust and user-friendly security solution. As these technologies continue to evolve, they are likely to play an increasingly important role in the future of identity and access management.

Biometric Type	Examples	Advantages	Challenges	Accuracy (EER*)
Physical Biometrics	Fingerprints, Facial Recognition, Iris Scans	High uniqueness, Stable over time	Requires specialized hardware, Privacy concerns	0.01% - 0.1%
Behavioral Biometrics	Typing Patterns, Mouse Movements, Gait Analysis	Continuous authentication, Passive monitoring	May vary with user state, Requires more data	2.46%

Table 1: Comparison of Physical and Behavioral Biometric Methods [3,5]

IV. Enhancing Security through Biometric and Behavioral Authentication

A. Multi-factor authentication (MFA) integration

The integration of biometric and behavioral authentication into multi-factor authentication (MFA) systems represents a significant advancement in security protocols. By combining biometrics with other authentication factors, such as passwords or tokens, organizations can create a more robust defense against unauthorized access. This layered approach significantly increases the difficulty for attackers to compromise user accounts, as they would need to bypass multiple, diverse security measures. For instance, a user might be required to provide a fingerprint scan in addition to a password, or facial recognition combined with a behavioral analysis of their typing patterns. The flexibility of biometric and behavioral methods allows for seamless integration into existing MFA frameworks, enhancing security without significantly impacting user experience.

B. Continuous authentication capabilities

One of the most powerful features of biometric and behavioral authentication is the ability to provide continuous, passive authentication throughout a user's session. Unlike traditional methods that typically authenticate users only at the point of login, these advanced techniques can constantly verify a user's identity based on their ongoing interactions with a system. This capability is particularly valuable in high-security environments or for protecting sensitive transactions. For example, behavioral biometrics can analyze a user's typing patterns, mouse movements, and application usage in real-time, detecting any anomalies that might indicate an unauthorized user has gained access to the system. This continuous monitoring provides an additional layer of security that goes beyond initial authentication, helping to prevent session hijacking and insider threats.

C. Comparison with traditional security measures

When compared to traditional security measures, biometric and behavioral authentication offer several distinct advantages:

1. Improved accuracy: Biometric methods generally provide higher accuracy rates than password-based systems, reducing the risk of false positives and negatives.
2. Resistance to common attacks: Unlike passwords, biometric data is much more difficult to steal, guess, or replicate, making it resistant to phishing, brute-force attacks, and social engineering tactics.
3. User convenience: Biometric authentication often requires less user effort than remembering and entering complex passwords, leading to improved user adoption and satisfaction.
4. Dynamic security: Behavioral biometrics, in particular, offer dynamic security that adapts to changes in user behavior over time, providing a more flexible and robust security solution.
5. Reduced administrative overhead: Biometric systems can decrease the need for password resets and account recovery processes, lowering IT support costs.

However, it's important to note that biometric and behavioral authentication are not without challenges. Privacy concerns, the need for specialized hardware in some cases, and the potential for false rejections in certain environments must be carefully considered and addressed.

Research has shown the effectiveness of these advanced authentication methods in enhancing security. A comprehensive study by Bhatt and Santhanam demonstrated that a multi-modal biometric system combining fingerprint, face, and iris recognition achieved an impressive 99.98% accuracy rate, significantly outperforming traditional single-factor authentication methods [6]. This high level of accuracy, combined with the ability to provide continuous authentication, positions biometric and behavioral methods as powerful tools in the ongoing battle against cyber threats.

As organizations continue to face evolving security challenges, the integration of biometric and behavioral authentication into comprehensive IAM strategies offers a promising path forward, balancing enhanced security with improved user experience.

V. Security Benefits of Biometric and Behavioral Authentication

A. Resistance to phishing and social engineering

Biometric and behavioral authentication methods offer strong resistance to phishing and social engineering attacks, which are among the most common and effective techniques used by cybercriminals. Unlike passwords or security questions that can be tricked out of users through deceptive emails or phone calls, biometric data is inherently tied to an individual's physical or behavioral characteristics. This makes it extremely difficult for attackers to obtain or replicate through social engineering tactics. For instance, a phishing email cannot convince a user to divulge their fingerprint or facial structure, nor can it mimic the complex behavioral patterns analyzed by advanced authentication systems.

B. Mitigation of credential theft and sharing

The use of biometric and behavioral authentication significantly reduces the risks associated with credential theft and sharing. Traditional passwords can be stolen through various means, including data breaches, keylogging, or simple observation. Once stolen, these credentials can be easily used by unauthorized individuals. In contrast, biometric data is much more challenging to steal or replicate. Even if biometric data is somehow compromised, many modern systems use techniques like template protection and encryption to render the stolen data unusable. Additionally, the unique nature of biometrics discourages credential sharing, a common security risk in environments where users might share passwords with colleagues or family members.

C. Real-time anomaly detection

One of the most powerful features of behavioral biometric systems is their ability to perform real-time anomaly detection. These systems continuously monitor user behavior patterns, such as typing rhythms, mouse movements, or application usage, and can quickly identify deviations from established norms. This capability allows for the detection of potential security breaches even after initial authentication has occurred. For example, if an authorized user's account is accessed by someone with significantly different behavioral patterns, the system can flag this as a potential security threat and trigger additional verification measures or alert security personnel.

D. Insider threat reduction

Insider threats, whether malicious or accidental, pose a significant risk to organizations. Biometric and behavioral authentication can play a crucial role in mitigating these risks. By providing continuous authentication throughout a user's session, these systems can detect unusual behavior that might indicate an insider threat. For instance, if an employee attempts to access resources outside their normal pattern or exhibits behavior inconsistent with their usual working style, the system can immediately flag this for investigation. This real-time monitoring and anomaly detection capability provides a level of security that goes beyond what traditional authentication methods can offer.

The effectiveness of biometric and behavioral authentication in enhancing security has been demonstrated in various studies. A comprehensive analysis by Sundararajan and Woodard examined the security benefits of behavioral biometrics, particularly in the context of continuous authentication. Their research showed that behavioral biometric systems could achieve error rates as low as 0.1% in controlled environments, providing a powerful tool for detecting unauthorized access and insider threats. The study also highlighted the potential of these systems to adapt to gradual changes in user behavior over time, maintaining high security while reducing false alarms [7].

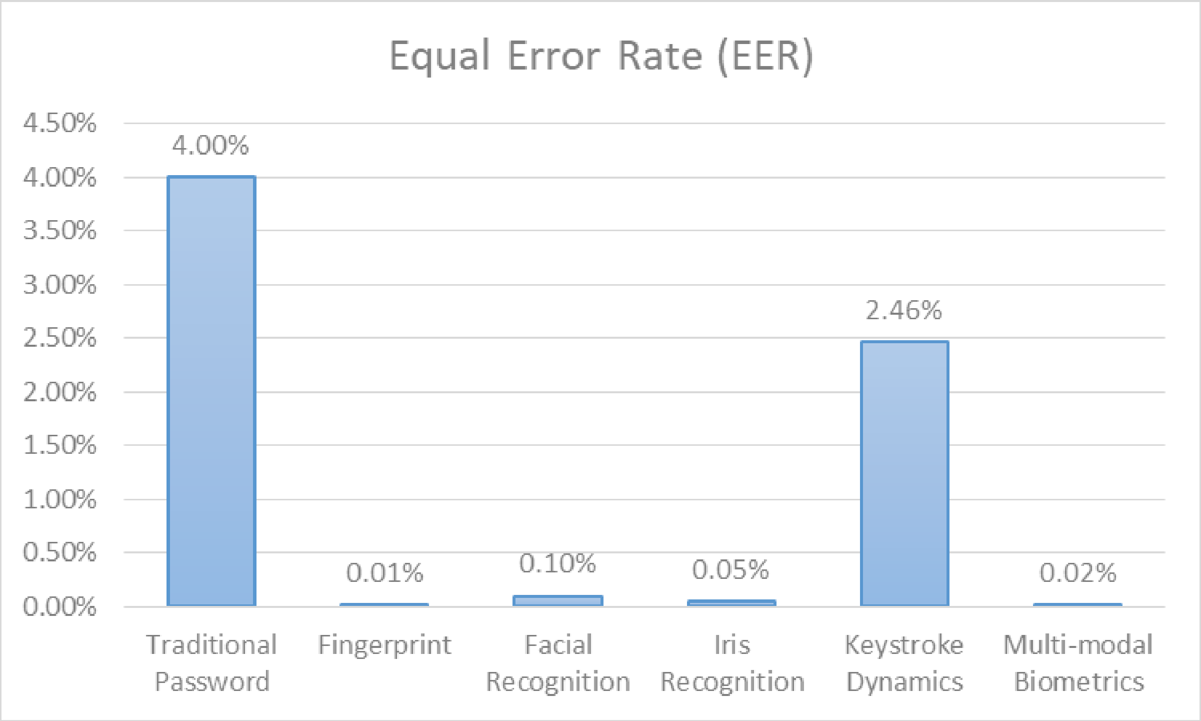


Fig 1: Accuracy Comparison of Authentication Methods [3-5]

As organizations continue to face increasingly sophisticated cyber threats, the adoption of biometric and behavioral authentication offers a robust defense against a wide range of attack vectors. By leveraging the unique characteristics of individuals, these advanced authentication methods provide a level of security that is difficult to circumvent through traditional hacking techniques. However, it's important to note that while these methods offer significant security benefits, they should be implemented as part of a comprehensive, layered security strategy to ensure the best possible protection against evolving cyber threats.

Benefit	Description	Impact
Phishing Resistance	Difficult to replicate biometric data through social engineering	Significant reduction in successful phishing attacks
Credential Theft Mitigation	Biometric data is harder to steal and use than passwords	Decreased risk of unauthorized access due to stolen credentials
Real-time Anomaly Detection	Continuous monitoring of user behavior patterns	Early detection of potential security breaches
Insider Threat Reduction	Ability to detect unusual behavior even after initial authentication	Enhanced protection against malicious insider activities
Improved Accuracy	Higher accuracy rates compared to password-based systems	Reduced false positives and negatives (up to 99.98% accuracy)

Table 2: Security Benefits of Biometric and Behavioral Authentication [6]

VI. User Experience and Convenience Factors

A. Reduction in password-related issues

The implementation of biometric and behavioral authentication significantly reduces password-related issues that have long plagued both users and IT departments. Password fatigue, resulting from the need to remember multiple complex passwords, often leads to poor security practices such as password reuse or the use of easily guessable passwords. Biometric authentication eliminates these problems by relying on inherent physical or behavioral characteristics. Users no longer need to remember complex strings of characters or frequently change their passwords, which not only enhances security but also improves the overall user experience. Additionally, the reduction in password-related help desk tickets, such as account lockouts and password resets, can lead to significant cost savings for organizations and improved productivity for IT staff.

B. Streamlined authentication processes

Biometric and behavioral authentication methods offer a more streamlined and efficient authentication process compared to traditional password-based systems. With biometrics, users can often authenticate themselves with a single action, such as a fingerprint scan or facial recognition, which is typically faster and more convenient than typing in a password. This streamlined process is particularly beneficial in environments where frequent authentication is required, such as healthcare settings or financial institutions. The speed and ease of biometric authentication can lead to improved workflow efficiency and user satisfaction. For example, a healthcare professional can quickly access patient records using a fingerprint scan, saving valuable time in critical situations.

C. Passive and continuous authentication benefits

One of the most significant advantages of behavioral biometrics is the ability to provide passive and continuous authentication. Unlike traditional methods that require explicit user action at specific intervals, behavioral biometrics can continuously verify a user's identity based on their ongoing interactions with a system. This approach offers several benefits:

1. Enhanced security: Continuous authentication can detect unauthorized access attempts in real-time, even if the initial login was legitimate.
2. Improved user experience: Users are not interrupted by frequent re-authentication requests, allowing for a seamless and uninterrupted workflow.
3. Contextual awareness: Behavioral biometrics can adapt to different contexts, potentially adjusting security levels based on the user's location, device, or activity.
4. Fraud detection: Unusual patterns in user behavior can be flagged for further investigation, helping to prevent fraud or insider threats.

The combination of these user experience and convenience factors makes biometric and behavioral authentication particularly attractive for both organizations and end-users. A study examined user perceptions and experiences with biometric authentication on mobile devices. Their findings indicated that users generally found biometric methods, particularly fingerprint recognition, to be more usable and less time-consuming than traditional PINs or passwords. The study also highlighted that users perceived biometric authentication as more secure, leading to increased trust in the technology [8].

As biometric and behavioral authentication technologies continue to evolve, we can expect further improvements in accuracy, speed, and user acceptance. However, it's crucial for organizations implementing these technologies to carefully consider the balance between security and usability, ensuring that the enhanced security measures do not come at the cost of a poor user experience. By thoughtfully integrating biometric and behavioral authentication into their security strategies, organizations can significantly enhance both their security posture and user satisfaction.

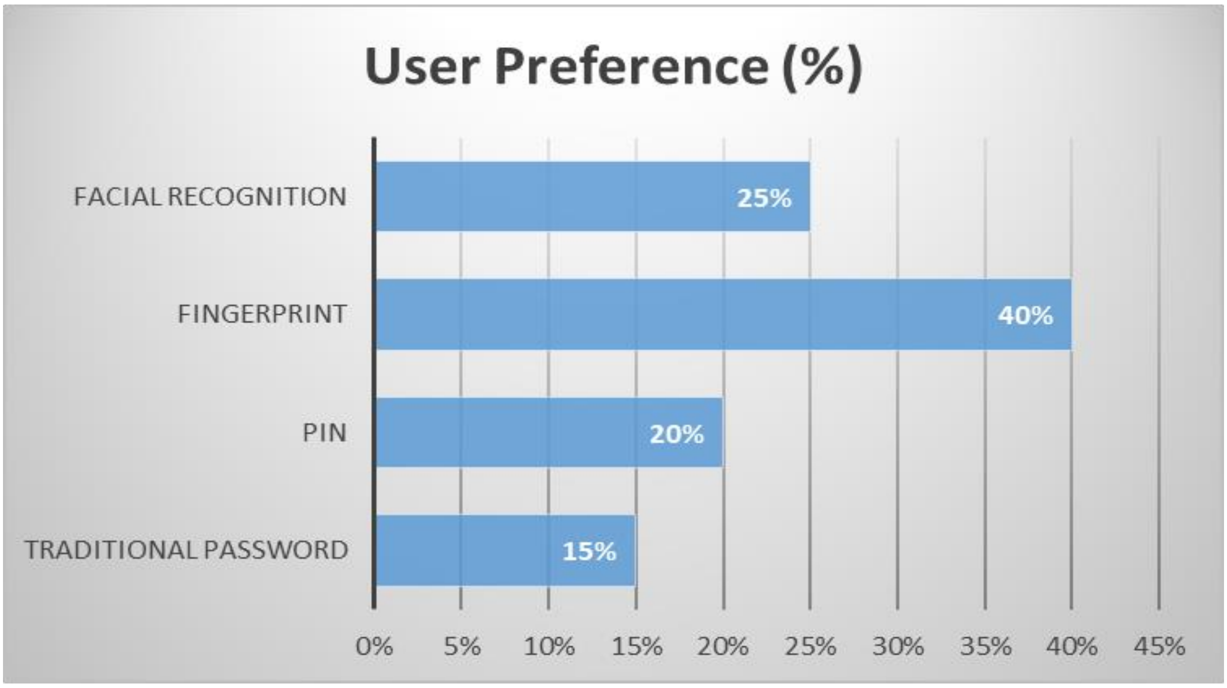


Fig 2: User Perception of Authentication Methods [8]

VII. Challenges and Considerations

A. Privacy concerns

The adoption of biometric and behavioral authentication raises significant privacy concerns. Unlike passwords, biometric data is inherently tied to an individual's identity and cannot be changed if compromised. This uniqueness makes biometric data a valuable target for cybercriminals and raises questions about potential misuse. Organizations must carefully consider the ethical implications of collecting and storing such sensitive personal information. Additionally, there are concerns about the potential for unauthorized surveillance or tracking of individuals through their biometric data [3].

B. Data security and storage

Securing biometric and behavioral data is crucial to maintaining the integrity of these authentication systems. The storage and transmission of this sensitive information require robust encryption and secure protocols to prevent unauthorized access or data breaches. Organizations must also comply with various data protection regulations, such as GDPR in Europe or CCPA in California, which impose strict requirements on the handling of personal data. Implementing proper data governance frameworks and regularly auditing security measures are essential to mitigate risks associated with biometric data storage [9].

C. Accuracy and false positive/negative rates

While biometric and behavioral authentication methods have significantly improved in recent years, accuracy remains a critical consideration. False positives (incorrectly granting access to an unauthorized user) and false negatives (incorrectly denying access to an authorized user) can have serious consequences for both security and user experience. Environmental factors, such as lighting conditions for facial recognition or background noise for voice authentication, can affect accuracy. Organizations must carefully calibrate their systems to balance security requirements with usability, considering the specific needs of their environment and user base [10].

D. Scalability and integration with existing systems

Implementing biometric and behavioral authentication at scale presents challenges, particularly for large organizations with complex IT infrastructures. Integrating these new authentication methods with existing identity and access management systems requires careful planning and potentially significant infrastructure upgrades. Organizations must consider factors such as compatibility with legacy systems, the need for specialized hardware (e.g., biometric scanners), and the impact on network performance. Additionally, ensuring consistent performance and security across diverse environments, including remote and mobile settings, adds another layer of complexity to scalability considerations.

VIII. Future Directions and Research Opportunities

A. Advancements in biometric technologies

The field of biometrics is rapidly evolving, with ongoing research into new modalities and improved accuracy. Emerging technologies such as vein pattern recognition, electrocardiogram (ECG) biometrics, and DNA-based authentication show promise for future applications. Additionally, advancements in sensor technologies are enabling more accurate and less intrusive biometric data capture. Research is also focused on developing more robust liveness detection methods to prevent spoofing attacks, such as the use of 3D facial recognition or multi-spectral imaging for fingerprint scanners [9].

B. Machine learning and AI in behavioral analysis

The application of machine learning and artificial intelligence in behavioral biometrics is a rapidly growing area of research. These technologies have the potential to significantly enhance the accuracy and adaptability of behavioral authentication systems. AI algorithms can analyze complex patterns in user behavior, learning and adapting to gradual changes over time while still detecting anomalies that may indicate security threats. Future research in this area is likely to focus on developing more sophisticated models that can handle a wider range of behavioral inputs and provide more nuanced risk assessments [9].

C. Context-aware authentication systems

The development of context-aware authentication systems represents an exciting frontier in IAM research. These systems aim to dynamically adjust authentication requirements based on contextual factors such as location, device type, time of day, and user activity patterns. By considering these contextual cues, authentication systems can provide a more flexible and user-friendly experience while maintaining high security standards. Research in this area includes the development of adaptive multi-factor authentication frameworks that can seamlessly integrate biometric, behavioral, and contextual data to make real-time authentication decisions [10].

As the field of biometric and behavioral authentication continues to evolve, addressing these challenges and pursuing these research opportunities will be crucial in realizing the full potential of these technologies for enhancing cybersecurity and improving user experiences.

Conclusion

In conclusion, the integration of biometric and behavioral authentication into Identity and Access Management systems represents a significant leap forward in cybersecurity. These advanced technologies offer robust solutions to many of the vulnerabilities inherent in traditional password-based systems, providing enhanced security, improved user experience, and greater resilience against evolving cyber threats. As we have explored, the benefits of these authentication methods are substantial, ranging from resistance to phishing and social engineering to the capability for continuous, passive authentication. However, the adoption of these technologies also brings challenges, particularly in areas of privacy, data security, and system integration. As research continues to advance, we can anticipate further improvements in accuracy, adaptability, and contextual awareness of biometric and behavioral authentication systems. The future of IAM lies in the thoughtful integration of these technologies, balanced with careful consideration of privacy and ethical concerns. Organizations that successfully navigate these challenges and leverage the power of biometric and behavioral authentication will be well-positioned to protect their digital assets and user identities in an increasingly complex cyber landscape. As we move forward, continued research and development in this field will be crucial in shaping the next generation of secure, user-friendly authentication systems, ultimately contributing to a more robust and resilient digital ecosystem.

References

1. S. Morgan, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," Cybercrime Magazine, Nov. 13, 2020. [Online]. Available: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/
2. Ghadeer Ibrahim Maki and Sarah Basim Abed, “Multimodal Biometric System Fusion Using Fingerprint and Iris with Convolutional Neural Network”, etj, vol. 9, no. 9, pp. 5140–5147, Sep. 2024. Online]. Available: https://everant.org/index.php/etj/article/view/1535
3. A. K. Jain, K. Nandakumar, and A. Ross, "50 years of biometric research: Accomplishments, challen-

ges, and opportunities," Pattern Recognition Letters, vol. 79, pp. 80-105, Aug. 2016. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0167865515004365

4. J. Daugman, "Information Theory and the IrisCode," IEEE Transactions on Information Forensics and Security, vol. 11, no. 2, pp. 400-409, Feb. 2016. [Online]. Available: https://ieeexplore.ieee.org/document/7328287
5. A. Alsultan, K. Warwick, and H. Wei, "Non-conventional keystroke dynamics for user authentication," Pattern Recognition Letters, vol. 89, pp. 53-59, Apr. 2017. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0167865517300429
6. T. Barbu, A. Ciobanu and M. Luca, "Multimodal biometric authentication based on voice, face and iris," 2015 E-Health and Bioengineering Conference (EHB), Iasi, Romania, 2015, pp. 1-4, doi: 10.1109/EHB.2015.7391373. [Online]. Available: https://ieeexplore.ieee.org/document/7391373
7. K. Sundararajan and D. L. Woodard, "Deep Learning for Biometrics: A Survey," ACM Computing Surveys, vol. 51, no. 3, pp. 1-34, May 2018. [Online]. Available: https://dl.acm.org/doi/10.1145/3190618
8. C. Bhagavatula, B. Ur, K. Iacovino, S. M. Kywe, L. F. Cranor, and M. Savvides, "Biometric Authentication on iPhone and Android: Usability, Perceptions, and Influences on Adoption," Proceedings of the NDSS Workshop on Usable Security, Feb. 2015. [Online]. Available: https://www.ndss-symposium.org/wp-content/uploads/2017/09/01_3_3.pdf
9. F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, "Quality Measures in Biometric Systems," IEEE Security & Privacy, vol. 10, no. 6, pp. 52-62, Nov.-Dec. 2012. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6095497
10. A. Lumini and L. Nanni, "Overview of the combination of biometric matchers," Information Fusion, vol. 33, pp. 71-85, Jan. 2017. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S1566253516300446