Cybersecurity and Innovation Technology Journal, Vol.3, No.1, 2025, pp. 9-16
e-ISSN 3025-6682. DOI. 10.52889/citj.v3i1.617

# Behavioral Biometrics for Healthcare Cybersecurity

Submitted 13 April 2025, Revised Date 26 April 2025, Accepted 27 April 2025

Maurice L. McBride[1,2*], Kenna L. Young[3]

[1]Healthcare Cybersecurity Program, Department of Healthcare Technology,
Capitol Technology University, Laurel, United States

[2]McBride Business Solutions, Columbia, United States

[3]3 Fold Ventures, Florida, United States
Corresponding Email: *mmcbride@captechu.edu

Abstract

With patient records going online, healthcare organizations are facing new-age threats and old-world security solutions. Typing, mouse, and voice dynamics are continuous and non-intrusive user authentication, enhancing security in clinical systems. This paper discusses the application of behavioral biometrics in mitigating insider threats, compromised credentials, and unauthorized access in the healthcare sector. The paper utilizes peer-reviewed articles published between 2020 and 2025 and applies thematic analysis to identify patterns, advantages, and disadvantages. Studies reveal that behavioral biometrics enhances identification, reduces system vulnerabilities, and can be easily integrated into existing systems. However, issues remain regarding algorithm bias, user privacy, and the system's sensitivity. The article concludes that while behavioral biometrics cannot be an effective substitute for conventional security measures, they are a valuable addition to IT security in the rapidly growing field of digital healthcare and can help healthcare facilities meet regulatory requirements.

Keywords: Behavioral Biometrics, Healthcare Cybersecurity, User Authentication, Insider Threats, Data Privacy

## INTRODUCTION

Security has become a critical issue in healthcare, where patient-related information is processed and transmitted electronically. Nevertheless, modern encryption, firewalls, and access control systems have not prevented cybercriminals from targeting healthcare organizations; the latter is valuable to cybercriminals because EHRs are worth significant money on the black market. Conventional security measures are inadequate for containing insider threats, stolen credentials, and social engineering attacks. This reality underscores the importance of adopting new technologies, such as behavioral biometrics, to enhance cybersecurity in the healthcare system.

Behavioral biometrics involves using behavior patterns, such as typing, mouse movements, walking, and voice, to identify and authenticate users continuously. Compared to more traditional biometrics, such as fingerprints or retina scans, behavioral biometrics offers a continuous form of user authentication that can enhance the real-time threat identification process without interrupting the user's tasks (Finnegan *et al.,* 2024). This paper discusses the following questions: What is behavioral biometrics, how can it improve cybersecurity in the healthcare sector, and what are its current prospects?

### *The Growing Threat Landscape in Healthcare Cybersecurity*

The healthcare industry is one of the sectors that frequently experience cyberattacks by cybercriminals. Alder (2024) reported that health records breaches exceeded 90 million in 2022 because of stolen credentials combined with phishing scams. These breaches expose medical patient information and insurance records combined with treatment documentation, causing damage to both healthcare facilities and their patients.

The Health Service Executive of Ireland became the victim of a ransomware attack that shut down their system for weeks, demonstrating the weak points of digital health systems (Muthuppalaniappan & Stevenson, 2020). Most data breaches result from malicious and accidental insider threats and cases of stolen credentials and phishing scams (Inayat *et al.,* 2024). Due to these challenges, it is necessary to have tools that can adapt to the context and quickly identify an intrusion, even if the login information is authentic.

Standard security measures are primarily based on borders and passwords that can be easily breached. Intrusion enablers reveal that lateral movement through a network is usually not easily detected after compromising a target. Behavioral biometrics is an additional layer of protection based on the analysis of a user’s behavior, which helps prevent various threats.

### *Understanding Behavioral Biometrics*

Behavioral biometrics can be defined as the process of measuring an individual's physical and behavioral characteristics for identification or verification. In contrast to physical biometrics, behavioral traits do not require touching; they cannot be easily faked and can be used for continuous authentication. These consist of typing rhythm, touches, navigation, voice pitch, and gait (Liang & Hamzah, 2025). In behavioral biometric systems, machine learning techniques are typically used to create user models. When a user enters the healthcare system to access information, the system verifies login credentials and examines user behavior to ensure the correct identity of the user (Ghilom & Latifi, 2024). In the event of such signs of an abnormal change in typing speed or navigation, access may be restricted or reviewed. Within a healthcare facility where many employees may use the same equipment, behavioral biometrics is a form of security that does not require the user to input a password. This can help achieve the goal of accountability and traceability in clinical settings without requiring logins and verification every time (Shojaei *et al.,* 2024).

### *Applications of Behavioral Biometrics in Healthcare Systems*

Behavioral biometrics is being implemented in several areas of healthcare security. The most critical application is the constant identification of the healthcare professionals who use the EHR systems (Basil *et al.,* 2024). For instance, consider a nurse who opens a patient file, and immediately, the file's behavior is different. For example, if the speed is high or the movement is jerky, then the system can alert or deny access. One of them is remote patient monitoring (RPM). Through behavioral biometrics, it is possible to ensure that the patient information is correctly associated with the individual using telehealth services or medical wearable devices (Ko *et al.,* 2023). This is especially important in the care of the elderly or patients with some level of dementia that would necessitate the need for a caregiver. Additionally, behavioral biometrics can be utilized in fraud detection for insurance claims and prescription monitoring programs, as Zhang *et al.* (2025) noted. The analysis of form submission data and login activities leads to fraud detection before behaviors become severe, according to Progonov *et al.* (2022).

### ***Advantages and Challenges of Implementation***

The implementation of behavioral biometrics in healthcare cybersecurity systems provides multiple advantageous features. The first is increased security through constant and non-intrusive user identification (Zhang *et al.,* 2024). Behavioral biometrics are less intrusive than fingerprint scans and, therefore, more suitable for clinical settings with high activity levels. This characteristic also makes it more difficult to spoof or perform social engineering attacks, as behavioral patterns cannot be easily emulated (Sarkar & Shukla, 2023).

Another advantage of using this software is its real-time detection of threats. Behavioral biometrics can enable systems to immediately alert and act on abnormalities, preventing threats (Subash & Song, 2021). In addition, these systems can be easily interfaced with existing authentication frameworks, making them flexible and scalable. However, challenges remain. One is the privacy and protection of data in line with current laws and regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) (Edemekong *et al.,* 2024). The behavioral data, including the results of its processing, must be secured to the maximum extent possible. Another problem is algorithmic bias, meaning some users may be incorrectly classified due to their behavior or disability. Lastly, false positives and the system's sensitivity may become an issue for the user if not correctly set (Van Giffen *et al.,* 2022).

### ***Comparative Analysis: Traditional vs. Behavioral Approaches***

However, passwords and multifactor authentication are traditional approaches that are commonly used and yet are gradually becoming insecure (Suleski *et al.,* 2023). Passwords can be cracked, snooped, or phished, and the MFA tokens can be intercepted or abused (Suleski *et al.,* 2023). Although these methods offer a level of protection, they do not account for the actions of authenticated users. Behavioral biometrics presents a viable solution, as it seeks to identify the user based on their behavior. Unlike other methods that only work at the time of login, behavioral biometrics works throughout the session. Thus, even if attackers gain access to the account, they cannot sustain the access for long (Balamurugan, 2024).

Furthermore, behavioral systems are more intelligent in context and capable of learning from user habits. For instance, it is possible that a clinician working at night exhibits different behavior from the same person working during the day, and adaptive systems can explain such changes. In this case, even though the traditional solutions remain relevant, behavioral biometrics add value by filling the gaps in post-login monitoring and insider threats (Alsowail & Al-Shehari, 2022).

## METHOD

### *Data Collection*

This research employed a secondary data research approach through a systematic literature review. The articles were collected from databases such as PubMed, IEEE Xplore, and ScienceDirect, and they all deal with behavioral biometrics in the context of healthcare cybersecurity. The studies sourced must have been published in English, under peer review, and been conducted within 5, meeting the following criteria.

The initial source list consisted of 200 sources, which were then screened for their applicability to healthcare, their contribution (empirical or theoretical), and the quality of the publication. Non-identified literature and research papers unrelated to healthcare were also excluded. This process provided 25 scholarly and government sources, which provide up-to-date information on the use of behavioral biometrics in cybersecurity.

### *Data Approach*

A cross-sectional study design was employed to sample the participants, and thematic analysis was used to categorize the patterns in the literature. These included authentication accuracy, usability, cyber incidents, and implementation challenges. This enabled structured comparisons across studies with different methodological approaches and results.

PRISMA guidelines consider all sources to ensure transparency and quality of work. The articles were coded using NVivo software to ensure the major themes could be easily distinguished and visualized. This supported the consistent identification of trends and synthesized implications for the use of behavioral biometrics in healthcare (Page *et al.,* 2021).

### *Justification of Approach*

A qualitative literature review was deemed suitable for the research question because behavioral biometrics is still emerging. Some are still in the pilot phase; hence, more emphasis is placed on secondary data from case studies, theoretical models, and simulations than full-scale trials.

This approach facilitated the integration and synthesis of knowledge from cybersecurity, healthcare IT, and ethics. This paper, which reviews various sources, helped gain different perspectives on the benefits, drawbacks, and requirements for using behavioral biometrics in healthcare facilities.

## RESULTS AND DISCUSSION

According to the literature discussed in this paper, it is evident that behavioral biometrics are beneficial in enhancing healthcare cybersecurity. Concerning the findings, it was established that behavioral biometrics yield very high results in user identification. Some investigations reveal that user identification rates exceeded 90%, according to Kumarapeli *et al.* (2024), as opposed to other mechanisms such as passwords or two-factor authentication. This high accuracy is due to the constant surveillance of behavioral characteristics, including typing, mouse movement, and even voice. Several of these systems have effectively identified users, thereby making the overall system more secure from unauthorized access.

Another highly relevant finding is the acceptance of behavioral biometric systems and practices, with impressions being overwhelmingly favorable. According to the study by Rukhiran *et al.* (2023), it is evident that systems that run invisibly in the background without requiring further verification are widely accepted. One of the most valuable aspects of these systems is that the installation is non-intrusive, which is particularly advantageous in fast-paced environments like healthcare facilities, where interruptions caused by service outages can directly impact healthcare delivery. These systems are, therefore, perceived as relatively easy to integrate into professional working practice without causing disruptive behavior changes of use, which has also contributed to their positive adoption by healthcare professionals.

However, like any other technological advancement, behavioral biometrics has some adverse effects. Some studies pointed out issues of over-detection, whereby accurate users were classified as technically suspicious. This issue becomes particularly crucial in clinical settings, where user behavior may fluctuate throughout the day or during periods of high or low workload. However, current studies promise the use of new and improved algorithms in machine learning that may help solve these problems. With advancements in machine learning models, the frequency of false alarms should decrease, and the system's ability to detect behavioral deviations also increases, thereby enhancing its applicability within actual clinical healthcare settings (Van Giffen *et al.,* 2022).

## CONCLUSION

Therefore, behavioral biometrics can be the new frontier of cybersecurity in the healthcare industry. These systems can identify attempts to bypass the authentication process, even when the traditional method is unsuccessful. According to Bajwa *et al.* (2021), healthcare is transforming digitally, necessitating innovative, intelligent security systems. Thus, it can help to minimize risks, protect remote working, and increase user responsibility. The main implementation challenges are linked to privacy and system tuning; however, there is no doubt that the advantages are significantly higher if the integration is meaningful.

## SUGGESTIONS

Establishing measures to reduce bias in behavioral biometric systems and performance studies for different population groups in the future is also key. The use of privacy-preserving technologies in machine learning, such as federated learning, can help address concerns about data sharing. Furthermore, small-scale implementation in large hospitals and other integrated health systems is also suggested to create a reference for the policy. Healthcare organizations should incorporate behavioral biometrics as a key measure in a comprehensive cybersecurity plan, including staff education, risk analysis, and compliance checks (Clarke & Martin, 2023). The next generation of cybersecurity will be centered around intelligent systems, and the future of these systems will lie in thinking, learning, and adapting to users' behavior.

## REFERENCES

Alder, S. (2024). Security Breaches in Healthcare in 2023. The HIPAA Journal, Michigan, United States. Available online: https://www. hipaajournal.com/security-breaches-in-healthcare/(accessed on December 2024).

Alsowail, R. A., & Al-Shehari, T. (2022). Techniques and Countermeasures for Preventing Insider Threats. PeerJ Computer Science, 8. https://doi.org/10.7717/peerj-cs.938

Bajwa, J., Munir, U., Nori, A., & Williams, B. (2021). Artificial Intelligence in Healthcare: Transforming the Practice of Medicine. Future Healthcare Journal, 8(2), 188–194. NCBI. https://doi.org/10.7861/fhj.2021-0095

Balamurugan, M. (2024). Biometric Authentication: A Double-Edged Sword for Security? International Journal of Science and Research (IJSR), 13(9), 170–173. https://doi.org/10.21275/sr24901230354

Basil, N., Ambe, S., Ekhator, C., & Fonkem, E. (2024). Health Records Database and Inherent Security Concerns: A Review of the Literature. Nih.gov. https://pmc.ncbi.nlm.nih.gov/articles/PMC9647912/

Clarke, M., & Martin, K. (2023). Managing cybersecurity risk in healthcare settings. Healthcare Management Forum, Vol. 37, No. 1. https://doi.org/10.1177/08404704231195804

Edemekong, P. F., Haydel, M. J., & Annamaraju, P. (2024). Health Insurance Portability and Accountability Act (HIPAA). National Library of Medicine. https://www.ncbi.nlm.nih.gov/books/NBK500019/

Ghilom, M., & Latifi, S. (2024). The Role of Machine Learning in Advanced Biometric Systems. Electronics, 13(13), 2667.. https://doi.org/10.3390/electronics13132667

Finnegan, O. L., White, J. W., Armstrong, B., Adams, E. L., Burkart, S., Beets, M. W., S. Nelakuditi, Willis, E. A., L. von Klinggraeff, Parker, H., Bastyr, M., Zhu, X., Zhong, Z., & Weaver, R. G. (2024). The utility of behavioral biometrics in user authentication and demographic characteristic detection: a scoping review. Systematic Reviews, vol. 13, no. 1. https://doi.org/10.1186/s13643-024-02451-1

Inayat, U., Farzan, M., Mahmood, S., Zia, M. F., Hussain, S., & Pallonetto, F. (2024). Insider threat mitigation: Systematic literature review. Ain Shams Engineering Journal, 103068. https://doi.org/10.1016/j.asej.2024.103068

Kumarapeli, D., Jung, S., & Lindeman, R. W. (2024). Privacy threats of behaviour identity detection in VR. Frontiers in Virtual Reality, 5, 1197547. https://doi.org/10.3389/frvir.2024.1197547

Ko, H. Y. K., Tripathi, N. K., Mozumder, C., Muengtaweepongsa, S., & Pal, I. (2023). Real-Time Remote Patient Monitoring and Alarming System for Noncommunicable Lifestyle Diseases. International Journal of Telemedicine and Applications, 2023, e9965226. https://doi.org/10.1155/2023/9965226

Liang, W., & Hamzah, F. (2025). Behavioral Biometrics and AI for Cloud User Authentication. https://www.researchgate.net/publication/389717394_Behavioral_Biometrics_and_AI_for_Cloud_User_Authentication/download

Muthuppalaniappan, M., & Stevenson, K. (2020). Healthcare Cyber-Attacks and the COVID-19 Pandemic: An Urgent Threat to Global Health. International Journal for Quality in Health Care, vol. 33, no. 1. https://doi.org/10.1093/intqhc/mzaa117

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., & McGuinness, L. A. (2021). The PRISMA 2020 statement: An updated Guideline for Reporting Systematic Reviews. British Medical Journal, 372(71). https://doi.org/10.1136/bmj.n71

Progonov, D., Cherniakova, V., Kolesnichenko, P., & Oliynyk, A. (2022). Behavior-based user authentication on mobile devices in various usage contexts. EURASIP Journal on Information Security, 2022, 1. https://doi.org/10.1186/s13635-022-00132-x

Rukhiran, M., Wong-In, S., & Netinant, P. (2023). User Acceptance Factors Related to Biometric Recognition Technologies of Examination Attendance in Higher Education: TAM Model. Sustainability, 15(4), 3092. https://doi.org/10.3390/su15043092

Sarkar, G., & Shukla, S. K. (2023). Behavioral Analysis of Cybercrime: Paving the Way for Effective Policing Strategies. Journal of Economic Criminology, 2(1), 100034. https://doi.org/10.1016/j.jeconc.2023.100034

Shojaei, P., Gjorgievska, E. V., & Chow, Y.-W. (2024). Security and Privacy of Technologies in Health Information Systems: A Systematic Review of the Literature. Computers, 13(2). https://doi.org/10.3390/computers13020041

Subash, A., & Song, I. (2021, November 1). Real-Time Behavioral Biometric Information Security System for Assessment Fraud Detection. IEEE Xplore. https://doi.org/10.1109/ICOCO53166.2021.9673568

Suleski, T., Ahmed, M., Yang, W., & Wang, E. (2023). A Review of Multi-Factor Authentication in the Internet of Healthcare Things. Digital Health, 9(1), 1–20. https://doi.org/10.1177/20552076231177144

Van Giffen, B., Herhausen, D., & Fahse, T. (2022). Overcoming the pitfalls and perils of algorithms: A classification of machine learning biases and mitigation methods. Journal of Business Research, 144(6), 93-106. https://doi.org/10.1016/j.jbusres.2022.01.076

Zhang, J., Liu, Z., & Luo, X. (Robert). (2024). Unraveling the Juxtaposed Effects of Biometric Characteristics on User Security Behaviors: A Controversial Information Technology Perspective. Decision Support Systems, 183, 114267. https://doi.org/10.1016/j.dss.2024.114267

Zhang, Z., Yin, H., Rao, S. X., Yan, X., Wang, Z., Liang, W., Zhao, Y., Shan, Y., Zhang, R., Lin, Y., & Jiang, J. (2025). Identifying E-Commerce Fraud Through User Behavior Data: Observations and Insights. Data Science and Engineering. https://doi.org/10.1007/s41019-024-00275-6