ISSN: 2976-7466

Journal of Biosensors and Bioelectronics Research

SCIENTIFIC Research and Community

Review Article

Open Access

Behavioral Biometrics for Continuous Authentication

Anvesh Gunuganti

USA

ABSTRACT

Gaining control over the security of the information and personal data stored in the devices has been crucial in the current digital world. Passwords and PINs, which are the common identity check methods at the beginning of the using phase of the devices, are less powerful once the devices themselves are in use. Transitioning to the second type, continuous authentication based on behavioral biometrics, becomes a strong solution to improve security throughout the session. This paper aims to discuss continuous authentication and its usage in coupling the behavioral components across computing devices. These recommendations underscore the successes of some of the methods, like keystroke dynamics and mouse movements, in ascertaining users' identities in real time. These are how the various platforms can work together and handle privacy-related issues. The future trends of studies focus on the necessity of improving the algorithms of biometric identification and increasing the adaptability of those algorithms to provide maximum protection in cyberspace.

***Corresponding author**

Anvesh Gunuganti, USA.

Received: August 10, 2023; **Accepted:** August 14, 2023; **Published:** August 26, 2023

Keywords: Behavioral Biometrics, Continuous Authentication, User Behavior Analysis, Biometric Authentication, Real-Time Monitoring

Abbreviations

PIN - Personal Identification Number
PCs - Personal Computers
AUC - Area Under the Curve
BB - Behavioral Biometrics

Introduction

With people using smartphones, tablets, laptops, and PCs in their day-to-day lives, the safety and privacy of information and data on all these digital gadgets have become a major concern. Limitations of the conventional Means of password and PIN, for example, are quite prominent in the sense that they do not provide sufficient security to the device once it is in use [1]. This vulnerability requires better security solutions to ensure the user's identity over their sessions on these devices is constantly validated. With the focus on continuous authentication as a novel method that will improve organizational security and protection of resources beyond the initial login stage, this paper examines the notion of behavioral biometrics. Fig. 1 explains 2 types of biometrics: Physiologic and Behavioral.

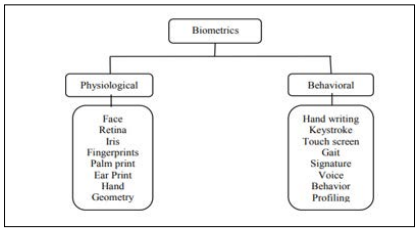

Figure 1: Approaches to Authenticate users using Biometrics [1]

Overview

This paper looks at different approaches and techniques of continuous authentication that use behavioral biometrics. It is also important to point out that there is a definition of behavioral biometrics referring to patterns of individuals' behavior, including typing patterns, mouse movements, and gesture dynamics. While previous or checkpoint authentication authenticates a user only at the initial login time, continuous authentication continues to periodically authenticate the user, reducing users' vulnerability to impersonation when using computers. In this way, detecting all these biometric behaviors with the help of devices and constant control and analysis allows users to recognize them with minimal interference in their work. It improves security by excluding the possibility of unauthorized access to confidential data.

Importance

The importance of the continuous authentication method can be summarized by the fact that they cancel out the limitations of static authentication methods. Continuous authentication is used where data security is paramount; it is common in business establishments or personnel gadgets storing sensitive data or information [2]. It is more secure because user identities are being dynamically verified through behavioral biometrics, which is the chief disadvantage; however, user convenience and productivity are unaffected. However, with the ever-new and developing risks and vulnerabilities, there is the need for constant authentication as it is one of the most effective approaches towards preventing new-age threats in cyberspace. Fig. 2 shows the process of continuous authentication.

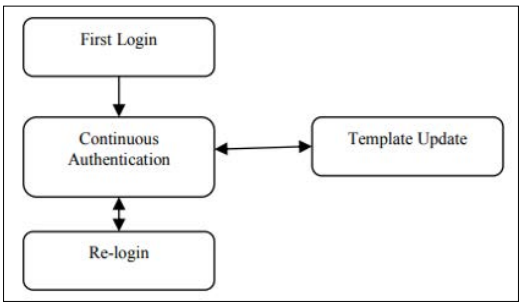

Figure 2: Process of Continuous Authentication [1]

Biometric Technique

- **Keystroke Dynamics**

Keystroke dynamics focus on characteristics in how a person types, both the speed at which they type and the time they take between keystrokes Another form of biometric means is based on checking particular users based on typing characteristics, which is highly efficient for real-time identification and, at the same time, does not interfere with ordinary work. It is very helpful when monitoring the environment is important, as it should be continuous to sustain security [3].

- **Mouse Dynamics**

Mouse dynamics refer to how the user utilizes the mouse or a touchpad, whether moving the mouse to shift focus, moving the cursor fast or slow, or clicking. This technique offers information concerning the route chosen for the individual client and is applied to affirm the user's identity without interruption [4]. It satisfies important criteria after keystroke dynamics and helps to strengthen the security system with another kind of behavioral data.

- **Gesture Recognition**

Gesture recognition involves sorting and analyzing particular movements or gestures made by the users, including movements made over touch surfaces or camera lenses. This one authenticates users using gesture signatures while integrating the physical functionality of touch to biometric identification. This method is normally incorporated in touch-based devices and applications where users' information is sensitive [5].

- **Voice Analysis**

Voice analysis is a biometric technology that looks at the acoustic features of an individual's voice, such as pitch, tone, and pronunciation. It authenticates the user by evaluating such vocal characteristics; thus, only users with the privileges to access voice-associated gadgets or services can do so [6]. This biometric technique is well suited to instances where voice commands and or communications are heavily used in the topic under consideration.

These biometric techniques use unique behaviors that provide security improvements and real-time authentication that continue to effectively identify the individual. These are reliable solutions to replace the conventional identity verification approach that is ineffective in most contexts. Fig. 3 explains a biometrics based mobile authentication framework

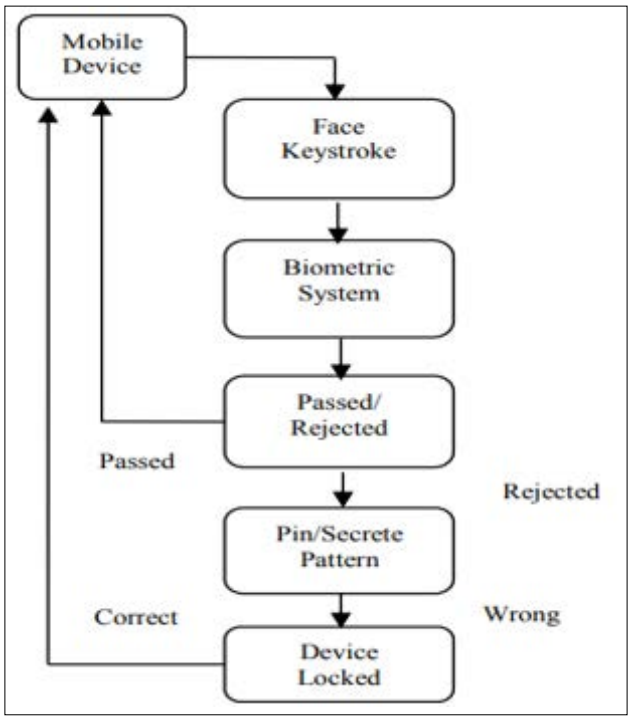

Figure 3: A Biometrics based Mobile Authentication Framework [1]

Aim of the Review

This paper will provide an extensive review of the state of research on behavioral biometrics that will enable continuous authentication on computing devices. It encompasses:

- Examination of Current Methods: A review of the current approaches in applying Behavioral Biometrics for constant authentication.
- Identification of Effective Biometric Traits: Evaluation of the best and most accurate biometric measures for repeated user identification.
- Proposal of Implementation Frameworks: To a large extent, uncovering the possible approaches and platforms that may be adopted for the natural integration of continuous authentication into commonplace computing devices.
- Discussion of Challenges and Limitations: Describing the possible shortcomings, disadvantages, and threats related to continually authenticating people.
- Exploration of Future Directions: Further research on future developments and new ideas on continuous authentication employing behavioral biometrics and trends and technologies in the field.

Thus, based on the analyzed aspects, the review is expected to shed light on the current state of continuous authentication and its applicability to strengthen cybersecurity protection in today's digital world.

Methodology

Information gathering for this review entails conducting a literature review to identify previous studies, conference proceedings, and technical papers on Behavioral Biometrics for Continuous Authentication and systematically extracting useful data from these sources. The main purpose of the research is to gather information concerning the techniques and solutions introduced for persistent user identification by using Behavioral Biometric techniques, focusing on security and ease of use.

This will involve determining the particular biometric features used in each study, methods of enrolment and authentication during the continuous process, the kind of datasets used for validation, and the comparisons made regarding their effectiveness. An issue of primary concern is thus to fill gaps in knowledge about how behavioral biometrics is implemented and how continuous authentication based on the discipline fares. This will be done by systematically gathering data from various sources and synthesizing information to extend knowledge and, possibly, create an integrated approach.

This systematic approach is anticipated to offer a significant understanding of the implications of behavioral biometrics on security and usability in authentication system

Table 1: PICOC TABLE

Keyword	Description
Behavioral biometrics	Study of unique user behavior patterns
Continuous authentication	Ongoing verification of user identity
User behavior analysis	Analysis of patterns in user actions
Biometric authentication	Identification using unique biological traits
Real-time monitoring	Continuous observation of user activities

Research Question

How can behavioral biometrics be effectively utilized for continuous authentication to enhance the security of devices beyond the initial login process?

Search Strategy

In the process of article selection, the keywords relevant across the databases and scholarly journals will be used, given the current trends related to the study. In this case, Grey literature will also be searched to get as many findings about the topic as possible, including books and articles not included in the list of peer-reviewed ones. Due to the desire to improve the specificity and depth of the results, a systematic search applying keywords and Boolean operators will be employed in the selected databases. The following databases will be searched:

- SpringerLink
- ScienceDirect
- IEEE

Keywords

- Behavioral biometrics
- Continuous authentication
- User behavior analysis
- Biometric authentication
- Real-time monitoring Search String:

("Behavioral Biometrics" OR "Behavioral Biometric Traits") AND "Continuous Authentication"

Inclusion and Exclusion Criteria

Inclusion Criteria

- Articles published in peer-reviewed journals or conference proceedings.
- Publication year between 2018 to 2022.
- Open-access articles only.
- Focus on Interoperability and Cross-Chain Security
- Relevance to the topic is evident in the title and abstract

Exclusion Criteria

- Publications outside the specified publication timeframe
- Articles without open access availability.
- Irrelevant to Interoperability and Cross-Chain Security as determined by title and abstract screen

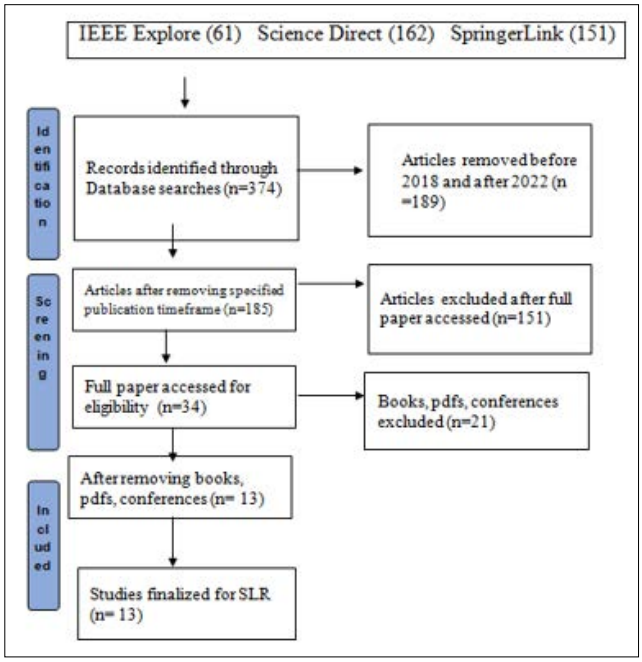

Figure 4: PRISMA Framework

Data Extraction

The information-gathering method for this review includes extracting data from research papers, conference proceedings, and technical reports, mainly on Behavioral Biometrics for Continuous Authentication. The emphasis is placed on identifying the techniques and solutions proposed for constant user authentication based on behavioral biometrics, which concerns security and usability.

The extraction process will involve defining the particular biometric technologies employed in each of the studies, approaches of continuous authentication, the data set used for the validation, and the comparative assessment of the effectiveness. There are concerns about the knowledge that has not covered the application of behavioral biometrics as a method of continuous authentication. This will be done by methodically translating the data from various forms and sources and categorizing them to build an understanding of and possibly unifying the field.

Table 2: Search Result

Sources	Total	Criteria 1	Criteria2	Criteria3	Final
Science Direct	162	74	12	11	11
IEEE	61	26	1	1	1
Springer Link	151	85	21	1	1

Data Synthesis

The synthesis on Behavioral Biometrics for Continuous Authentication reveals:

- **Biometric Techniques:** Recognition of better approaches such as keystroke dynamics, mouse dynamics, gesture recognition, and voice analysis for constant user verification.
- **Methodologies:** Continuous authentication schemes, that is, touch point-based strategies, and the considerations of the user experience and privacy during device interactions.
- **Validation and Metrics:** Using and studying scores and AUC to determine the system's accuracy and repeatability.
- **Comparative Analysis:** Assessment of possibilities and drawbacks of various biometric methods with influence on security and flexibility.
- **Integration and Applications:** Knowledge of how to apply BB in various fields such as finance, healthcare, and the government sector, focusing on compliance and privacy issues.
- **Challenges and Future Directions:** Challenges have been stated as apprehensive to user acceptance and variability in data, and ideas have been proposed to work on improving the algorithms and the sensors used.

Findings and Discussion

The review of Behavioral Biometrics for Continuous Authentication reveals several key insights and findings:

- **Effective Biometric Techniques:** Among the most successful trending biometrics, there are keystroke dynamics, mouse dynamics, and gesture recognition [7]. These techniques involve using features like typing speed, mouse movement, and gestures' dynamics and making immediate identifications of users, which provides better security than regular passwords or PINs.
- **Applications Across Industries:** Biometric behavior financing differs in offering services in various fields, such as financial, healthcare, and government departments [8]. In commerce, they offer protection in internet buying and selling and ensure that only authorized personnel gain access to the financial information. They protect the records that clients have and ensure that the facilities they work for do not infringe on the laws regarding patients' privacy. Some government uses it for classified data access and security from cybercriminals.
- **Performance Metrics and Validation:** Comparison of the various biometric modalities indicates the level of accuracy and reliability of each modality [9]. For example, keystroke dynamics are shown to have high accuracy in identifying users based on their typing behavior; however, the issues remain regarding controlling false acceptance and rejection rates with varying populations and conditions.
- **Challenges and Limitations:** While there are benefits of using behavioral biometrics, there are also drawbacks; for instance, users might not accept the idea of being monitored, biometric data may vary because of the surrounding environment, and lastly, behavioral biometrics are vulnerable to spoofing attacks [10]. Overcoming these obstacles is imperative to create the adoption and trust in continuous authentication processes using behavioral biometrics [11].
- **Future Research Directions:** As such, there are also implications for future research; these will include better machine learning algorithms in terms of biometric pattern recognition, improvements in the sensors used to gather more detailed behavioral data, and the creation of industry standards through the structured protocol to facilitate compatibility and security. That way, it is possible to look deeper into the potential of such applications and the possibility of using more than one biometric modality for continuously increased ease of use, security, acceptance, and robustness.
- **Implications for Security and Privacy:** As much as behavioral biometrics provides high-level security features, privacy and data protection are still major concerns. Further evolution should be focused on proving the ethical application of the technology and compliance with identified and future regulations regarding the protection of personal data and the process of obtaining users' consent.

Answering the Research Question

It is critical to protect devices given the day's interconnected world and emerging cyber threats, as this passage from Brave New World illustrates. It is worth emphasizing, however, that behavioral biometrics go beyond initial authentications, providing constant security measures using individuals' specific characteristics.

- **Continuous Authentication Need:** Behavioral biometrics help meet new security needs beyond initial logins and guarantee device security given the increasing threats. Fig. 5 explains different module of biometric authentication systems

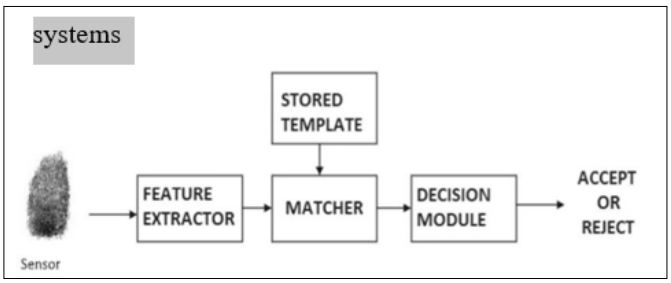

Figure 5: Different Module of Biometric Authentication Systems [11]

- **Unique Biometric Traits:** These may include the Keystroke dynamics and mouse movements that constantly validate the identity of the user and provide extremely enhanced security from intruders. Also in fig. 6 explains eight different points of attacks in biometric systems

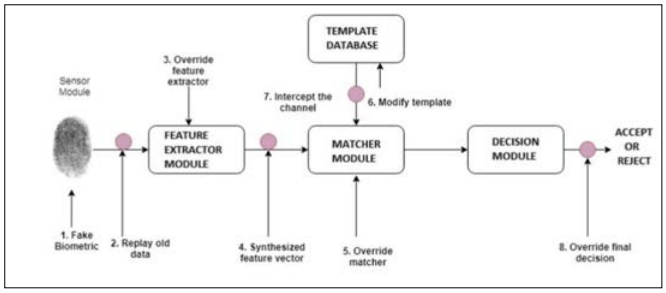

Figure 6: Eight different Points of Attacks in Biometric Systems [11]

- **Real-time Monitoring:** The implemented biometric systems continuously supervise the users' activity in real-time and can modify the security measures based on the identified threats.
- **Enhanced Security Postures:** Integrating binaural and gesture recognition further enhances the gadget's safeguard than conventional biometric systems.

Conclusion

Therefore, it is possible to conclude that behavioral biometrics as a means of continuous authentication is a significant leap forward in device protection from unauthorized access beyond

the basic login processes. Keystroke dynamics and mouse movements offer comfortable and constant user identity validation, improving security. Furthermore, bioAura and gesture recognition applications also enhance security stances since they incorporate more real-time confirmation steps that change with the user's activities. Thus, these biometric solutions eliminate the risks of static authentication types and provide strong protection against the modern network threats rampant in integrated digital systems.

Moving into the future, the continuous advance and implementation of behavioral biometrics show great potential for enhancing favorable security throughout numerous forms of industries. Over the years, technology development has increased, and new strategies for protecting individual and company information have also changed. By adopting these new-age biometric solutions into everyday products, institutions can strengthen their resistance to data breaches and identity theft. Future work in the field of biometric algorithms should aim at perfecting them, adapting them to the existing platforms, and solving the problem of privacy concerns so that the algorithms provided are as effective and helpful in protecting digital assets as possible.

Key Findings and Insights

Here are the key findings from the study on "Behavioral Biometrics for Continuous Authentication":

- **Enhanced Security Beyond Initial Logins:** Keystrokes and mouse movements, as examples of behavioral biometrics, enable continuous authentication services, which help protect devices beyond login processes.
- **Real-Time Monitoring and Adaptation:** Biometric systems pay attention to the details of the user's actions, constantly changing the level of security to prevent any threats, which makes the device's overall security high.
- **Effectiveness of Unique Biometric Traits:** BioAura and gesture recognition strengthen security outlooks by enhancing standard credentials' effectiveness to shield the systems against illegitimate attempts.
- **Integration Challenges and Privacy Considerations:** Despite such gains, difficulties in actively implementing behavioral biometrics can be observed, such as the compatibility issue where these technologies are not perfectly compatible with several platforms in use and privacy issues in constantly monitoring users' behaviors.
- **Future Directions and Research Opportunities:** More research and improvement of algorithms are needed to make the perfect recognition results, enhance accuracy, and reach the user's acceptance. Future research should aim to define common practices regarding biometrics for mobile platforms and improve compatibility to optimize the effectiveness of employing biometrics in the protection of digital space.

These outcomes reveal that behavioral biometrics can revolutionize the device protection process and stress the necessity of further growth in this sphere for today's changing cybersecurity demands.

References

1. J Handa, A Singh, A Goyal, P Aggarwal (2018) Behavioral Biometrics for Continuous Authentication. International Conference on Parallel Distributed and Grid Computing (PDGC) https://ieeexplore.ieee.org/document/8745880/metrics#metrics.
2. Y Liang, S Samtani, B Guo, Z Yu (2020) Behavioral Biometrics for Continuous Authentication in the Internet-of-Things Era: An Artificial Intelligence Perspective. IEEE Internet of Things Journal 7: 9128-9143.
3. G Stragapede, R Vera Rodriguez, R Tolosana, A Morales, A Acien, et al. (2022) Mobile behavioral biometrics for passive authentication. Pattern Recognition Letters 157: 35-41.
4. N Karakaya, GI Alptekin, ÖD İncel (2019) Using behavioral biometric sensors of mobile phones for user authentication. Procedia Computer Science 159: 475-484.
5. HC Volaka, G Alptekin, OE Basar, M Isbilen, OD Incel (2019) Towards Continuous Authentication on Mobile Phones using Deep Learning Models. Procedia Computer Science 155: 177-184.
6. D Hayes, F Cappa, NA Le Khac (2020) An effective approach to mobile device management: Security and privacy issues associated with mobile applications. Digital Business 1: 100001.
7. AG Martín, I Martín de Diego, A Fernández Isabel, M Beltrán, RR Fernández () Combining user behavioural information at the feature level to enhance continuous authentication systems. Knowledge Based Systems 244: 108544.
8. L Hernández Álvarez, JM de Fuentes, L González Manzano, L Hernández Encinas (2021) Smart CAMPP - Smartphone-based continuous authentication leveraging motion sensors with privacy preservation. Pattern Recognition Letters 147: 189-196.
9. PK Rayani, S Changder (2022) Continuous user authentication on smartphone via behavioral biometrics: a survey. Multimedia Tools and Applications 82: 1633-1667.
10. R Rocha, D Carneiro, R Costa, César Analide (2019) Continuous Authentication in Mobile Devices Using Behavioral Biometrics. Advances in intelligent systems and computing 191-198.
11. A Sarkar, BK Singh (2020) A review on performance, security and various biometric template protection schemes for biometric authentication systems. Multimedia Tools and Applications 79: 27721-27776.