IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 7, July 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307140|

Continuous Authentication and Behavioral Biometrics: Enhancing Cybersecurity in the Digital Era

Sailesh Oduri

Charles River Laboratories, USA

ABSTRACT: Continuous authentication and behavioral biometrics have emerged as promising solutions to address the limitations of traditional authentication methods in the face of increasingly sophisticated cybersecurity threats. This article explores the concepts, advantages, and real-world applications of these cutting-edge technologies, highlighting their potential to revolutionize user authentication and access control. By leveraging machine learning algorithms and analyzing user behavior in real-time, continuous authentication systems can detect anomalies and adapt security measures based on the perceived risk. The integration of behavioral biometrics, such as keystroke dynamics, mouse movements, and touchscreen gestures, enables the establishment of unique digital fingerprints for each user, enhancing the accuracy and robustness of the authentication process. The article discusses the key components and functionality of continuous authentication, the role of machine learning in anomaly detection, and the advantages of behavioral biometrics over traditional methods. It also examines the implementation considerations, including integration with existing security infrastructure, privacy concerns, and user acceptance. Real-world applications and case studies in financial services, healthcare, and government organizations demonstrate the practical benefits of these technologies. The article concludes by exploring future trends and research directions, such as advancements in machine learning and artificial intelligence, integration with Internet of Things (IoT) devices, and continuous authentication in cloud computing environments. This comprehensive overview emphasizes the importance of adopting proactive and adaptive security measures to safeguard sensitive data and assets in the ever-evolving digital landscape.

KEYWORDS: Continuous Authentication, Behavioral Biometrics, Cybersecurity, Machine Learning, Adaptive Security

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307140|

I. INTRODUCTION

In the rapidly evolving landscape of cybersecurity, traditional authentication methods such as passwords and tokens are increasingly proving inadequate in the face of sophisticated security threats [1]. Phishing attacks, credential theft, and other malicious activities have exposed the vulnerabilities of these static authentication mechanisms [2]. As organizations strive to protect their sensitive assets and data in the digital era, the need for more robust and adaptive security measures has become paramount [3].

Continuous authentication and behavioral biometrics have emerged as promising solutions to address the limitations of traditional authentication methods. These cutting-edge technologies offer a proactive approach to cybersecurity by continuously monitoring user behavior and context throughout the entire user session [1]. By leveraging machine learning algorithms and analyzing patterns of user interactions, continuous authentication systems can dynamically adapt security measures based on risk factors and anomalies [2].

The integration of behavioral biometrics into continuous authentication frameworks adds a layer of security. Behavioral biometrics analyze unique patterns of user behavior, such as typing cadence, mouse movements, and touchscreen gestures, to establish a digital fingerprint for each user [3]. This enables the detection of deviations from normal behavior, triggering authentication challenges or security alerts to prevent unauthorized access or fraudulent activities [1].

Moreover, continuous authentication offers organizations a more seamless and frictionless approach to authentication, enhancing user experience while strengthening security [2]. By authenticating users based on their ongoing behavior and interactions, continuous authentication systems reduce the need for intrusive authentication prompts or interruptions [3]. This balance between security and usability is crucial in today's digital landscape, where user convenience and satisfaction are essential factors in the adoption and effectiveness of security measures [1].

In this article, we will explore the concepts of continuous authentication and behavioral biometrics in detail, discussing their key components, functionality, and advantages over traditional authentication methods. We will examine the role of machine learning algorithms in anomaly detection and the integration of these technologies with existing security infrastructures. Additionally, we will delve into real-world applications and case studies, highlighting the potential benefits for industries such as financial services, healthcare, and government organizations. Finally, we will discuss future trends and research directions in the field of continuous authentication and behavioral biometrics, emphasizing the importance of proactive cybersecurity measures in safeguarding sensitive data and assets in the digital era.

II. CONTINUOUS AUTHENTICATION: A PROACTIVE APPROACH TO SECURITY

Continuous authentication is a proactive security approach that continuously monitors and verifies the identity of users throughout their entire session [4]. Unlike traditional authentication methods that rely on one-time login credentials, continuous authentication systems constantly assess the user's behavior, context, and interactions to ensure ongoing legitimacy [1]. The concept of continuous authentication is built on the premise that security should not be a single event but rather a continuous process that adapts to the changing risk factors and potential threats [3].

Continuous authentication systems comprise several key components that work together to provide robust security. These components include data collection modules, user behavior analysis engines, risk assessment frameworks, and adaptive authentication mechanisms [4]. The data collection modules gather various types of user data, such as keystrokes, mouse movements, touch gestures, and device interactions [2]. The user behavior analysis engines employ machine learning algorithms to process this data and establish a baseline of normal user behavior [1].

The risk assessment frameworks continuously evaluate the user's actions and context against the established baseline, calculating risk scores based on the level of deviation from normal behavior [3]. These risk scores are then used to trigger adaptive authentication measures, such as additional verification steps or access restrictions when the risk level exceeds predefined thresholds [4]. The adaptive nature of continuous authentication allows the system to dynamically adjust security measures based on the perceived risk, providing a more granular and context-aware approach to security [2].

Risk-based authentication is a key aspect of continuous authentication systems. It involves assessing the risk associated with each user session based on factors such as the user's behavior, device, location, and network environment [1]. By considering these contextual factors, the system can determine the appropriate level of authentication required for a

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307140|

particular session [4]. For example, if a user is accessing sensitive data from an unfamiliar device or location, the system may prompt for additional authentication steps, such as biometric verification or two-factor authentication [3].
Adaptive security measures are another crucial component of continuous authentication. These measures are dynamically triggered based on the calculated risk scores and predefined security policies [2]. Adaptive security measures can include actions such as prompting for additional authentication, limiting access to sensitive resources, or even terminating the user session if the risk level becomes too high [4]. The adaptability of these measures allows organizations to strike a balance between security and usability, providing a more seamless user experience while maintaining a robust security posture [1].

Characteristics	Traditional Authentication Methods	Continuous Authentication
Authentication Frequency	One-time, at login	Continuous, throughout the session
User Interaction	Active, requires user input	Passive, seamless
Security Level	Static, vulnerable to attacks	Dynamic, risk-based
User Experience	Intrusive, interrupts workflow	Frictionless, transparent
Adaptability	Limited, fixed security measures	High, context-aware

Table 1: Comparison of Traditional Authentication Methods and Continuous Authentication [16]

III. BEHAVIORAL BIOMETRICS: ESTABLISHING UNIQUE DIGITAL FINGERPRINTS

3.1. Types of Behavioral Biometrics

Behavioral biometrics encompasses a wide range of user-specific patterns and behaviors that can be used to establish a unique digital fingerprint [5]. These biometric modalities are based on how users interact with their devices and applications, providing a non-intrusive and continuous form of authentication [3]. Some of the most commonly used behavioral biometrics include keystroke dynamics, mouse movements, and touchscreen gestures [1].

3.1.1. Keystroke Dynamics

Keystroke dynamics refers to the unique patterns and rhythms exhibited by users when typing on a keyboard [6]. This behavioral biometric captures characteristics such as typing speed, dwell time (the duration a key is pressed), and flight time (the time between consecutive keystrokes) [3]. By analyzing these patterns, continuous authentication systems can identify users based on their distinctive typing styles, even if they are using the same device or keyboard [5].

3.1.2. Mouse Movements

Mouse movements provide another valuable source of behavioral data for continuous authentication [1]. This biometric modality captures the way users interact with their mouse, including movement speed, acceleration, click duration, and scrolling patterns [6]. By analyzing these mouse dynamics, the system can establish a unique profile for each user, enabling the detection of anomalous behavior that may indicate unauthorized access attempts [3].

3.1.3. Touchscreen Gestures

With the widespread adoption of mobile devices and touchscreens, touchscreen gestures have become an important behavioral biometric [5]. This modality captures the unique patterns and characteristics of user interactions on touchscreen devices, such as swipe speed, touch pressure, and gesture patterns [1]. By analyzing these gestures, continuous authentication systems can differentiate between legitimate users and potential impostors, providing an additional layer of security for mobile applications [6].

Behavioral Biometric Modality	Key Features
Keystroke Dynamics	Typing speed, dwell time, flight time
Mouse Dynamics	Movement speed, acceleration, click duration
Touchscreen Gestures	Swipe speed, touch pressure, gesture patterns
Gait Recognition	Walking speed, stride length, body movements
Voice Recognition	Pitch, tone, speaking rhythm

Table 2: Common Behavioral Biometric Modalities and Their Features [1-6]

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307140|

3.2. Machine Learning Algorithms for Anomaly Detection

Machine learning algorithms play a crucial role in the implementation of behavioral biometrics for continuous authentication [5]. These algorithms are used to analyze the collected behavioral data and establish a baseline of normal user behavior [3]. Anomaly detection techniques, such as one-class support vector machines (SVM), hidden Markov models (HMM), and deep learning approaches, are employed to identify deviations from the established baseline [1].

Machine learning algorithms continuously learn and adapt to the user's behavior over time, refining the behavioral profile and improving the accuracy of anomaly detection [6]. By leveraging these advanced algorithms, continuous authentication systems can effectively detect and respond to potential security threats in real-time, minimizing the risk of unauthorized access and data breaches [5].

3.3. Advantages of Traditional Biometric Methods

Behavioral biometrics offer several advantages over traditional biometric methods, such as fingerprints or facial recognition [1]. Unlike physical biometrics, behavioral biometrics are non-intrusive and can be collected continuously without requiring explicit user action [3]. This makes behavioral biometrics more user-friendly and less disruptive to the user experience [6].

Moreover, behavioral biometrics are more resistant to spoofing and imitation attacks compared to traditional biometrics [5]. While physical biometrics can be copied or replicated, behavioral patterns are inherently more difficult to mimic or forge [1]. The dynamic and contextual nature of behavioral biometrics adds an extra layer of security, making it more challenging for attackers to circumvent the authentication process [3].

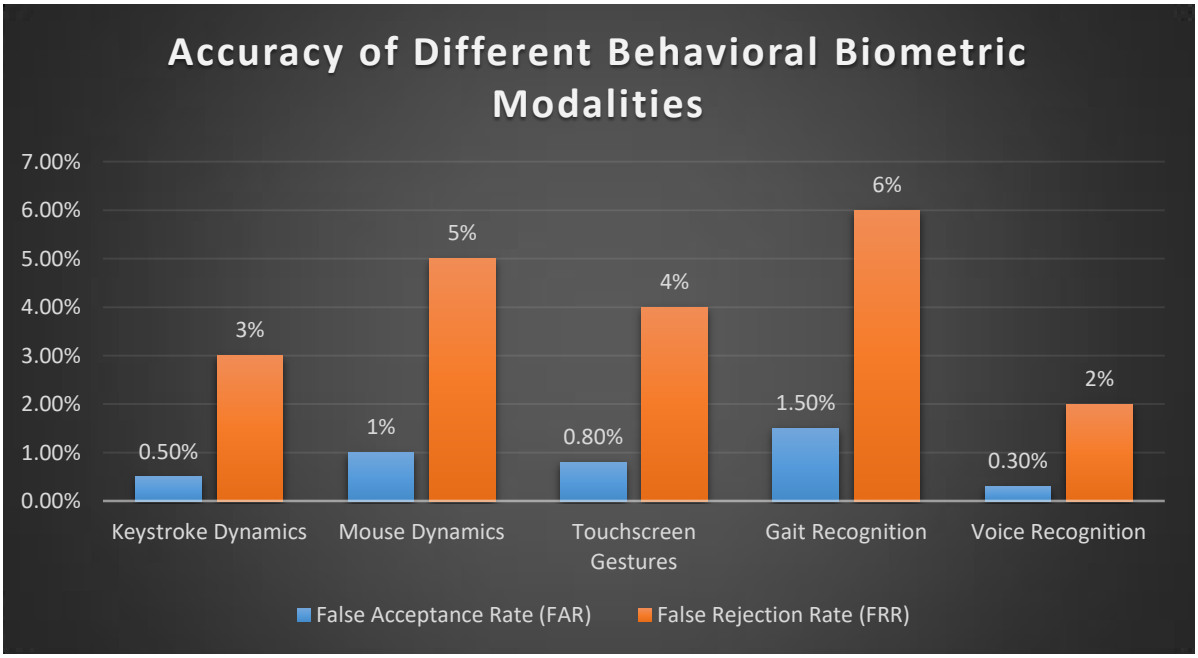

Figure 1: Accuracy of Different Behavioral Biometric Modalities [15]

IV. BALANCING SECURITY AND USER EXPERIENCE

4.1. Seamless and Frictionless Authentication

Continuous authentication aims to provide a seamless and frictionless user experience while maintaining a high level of security [7]. Traditional authentication methods often require users to actively participate in the authentication process, such as entering passwords or providing biometric data [5]. In contrast, continuous authentication operates in the background, continuously monitoring user behavior and context without requiring explicit user input [1].

By leveraging behavioral biometrics and machine learning algorithms, continuous authentication systems can transparently verify the user's identity throughout their session [8]. This approach minimizes user interruptions and

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307140|

eliminates the need for repetitive authentication steps, providing a more streamlined and user-friendly experience [7]. Users can focus on their tasks and interactions without being burdened by frequent authentication prompts, leading to increased productivity and satisfaction [5].

4.2. Reducing Authentication Fatigue and Interruptions

Authentication fatigue is a common problem faced by users in today's digital landscape [1]. The increasing number of accounts, services, and devices that require authentication can lead to user frustration and decreased productivity [7]. Continuous authentication addresses this issue by reducing the frequency and intrusiveness of authentication prompts [5].

By continuously monitoring user behavior and context, the system can maintain a persistent state of authentication, only prompting for additional verification when necessary [8]. This approach minimizes the number of interruptions users face during their sessions, reducing authentication fatigue and improving the overall user experience [1]. Users can seamlessly transition between tasks and applications without the constant need to re-authenticate, leading to a more efficient and satisfying interaction with the system [7].

4.3. Context-Aware Security and Adaptive Authentication

Context-aware security is a key aspect of continuous authentication that enables adaptive authentication measures based on the user's context and risk level [5]. By considering factors such as the user's location, device, network environment, and behavioral patterns, the system can dynamically adjust the authentication requirements to strike a balance between security and usability [1].

For example, if a user is accessing non-sensitive information from a trusted device and location, the system may allow seamless access without additional authentication [8]. However, if the user attempts to access sensitive data from an unfamiliar device or location, the system may prompt for stronger authentication, such as multi-factor authentication or biometric verification [7].

Adaptive authentication ensures that security measures are applied proportionately to the perceived risk, minimizing unnecessary friction for low-risk activities while enforcing stricter authentication for high-risk scenarios [5]. This context-aware approach enhances the user experience by providing a more personalized and risk-appropriate authentication process, reducing user frustration and increasing overall satisfaction [1].

V. IMPLEMENTATION CONSIDERATIONS

5.1. Integration with Existing Security Infrastructure

Implementing continuous authentication and behavioral biometrics requires careful consideration of the existing security infrastructure within an organization [9]. To ensure a smooth and effective deployment, it is essential to integrate these technologies with the current security systems, such as identity and access management (IAM) solutions, security information and event management (SIEM) platforms, and risk management frameworks [7].

Integration with IAM solutions enables the centralized management of user identities and access rights, allowing for the seamless incorporation of continuous authentication mechanisms [10]. SIEM platforms can be leveraged to collect and analyze behavioral data, providing real-time monitoring and alerting capabilities [9]. Risk management frameworks, such as the NIST Cybersecurity Framework, can guide the implementation process, ensuring alignment with industry best practices and regulatory requirements [7].

5.2. Privacy and Data Protection Concerns

The collection and processing of behavioral biometric data raise important privacy and data protection concerns [9]. As continuous authentication systems gather sensitive user information, it is crucial to address these concerns and ensure compliance with relevant regulations, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) [10].

Organizations must implement robust data protection measures, including secure storage, encryption, and access controls, to safeguard user data [7]. Transparent privacy policies and user consent mechanisms should be in place, informing users about the data being collected, its purpose, and how it will be used [9]. Regular audits and assessments should be conducted to ensure ongoing compliance and identify potential privacy risks [10].

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307140|

5.3. User Acceptance and Education

User acceptance and education play a vital role in the successful implementation of continuous authentication and behavioral biometrics [7]. While these technologies offer enhanced security and usability, users may have concerns about privacy and the monitoring of their behaviors [9]. To foster user acceptance, organizations must engage in clear communication and education efforts [10].

Users should be informed about the benefits of continuous authentication, such as improved security and reduced authentication friction [7]. Transparent explanations should be provided regarding the types of behavioral data being collected, how it is used, and the measures in place to protect user privacy [9]. Training programs and user guides can help users understand the authentication process and their role in maintaining security [10].

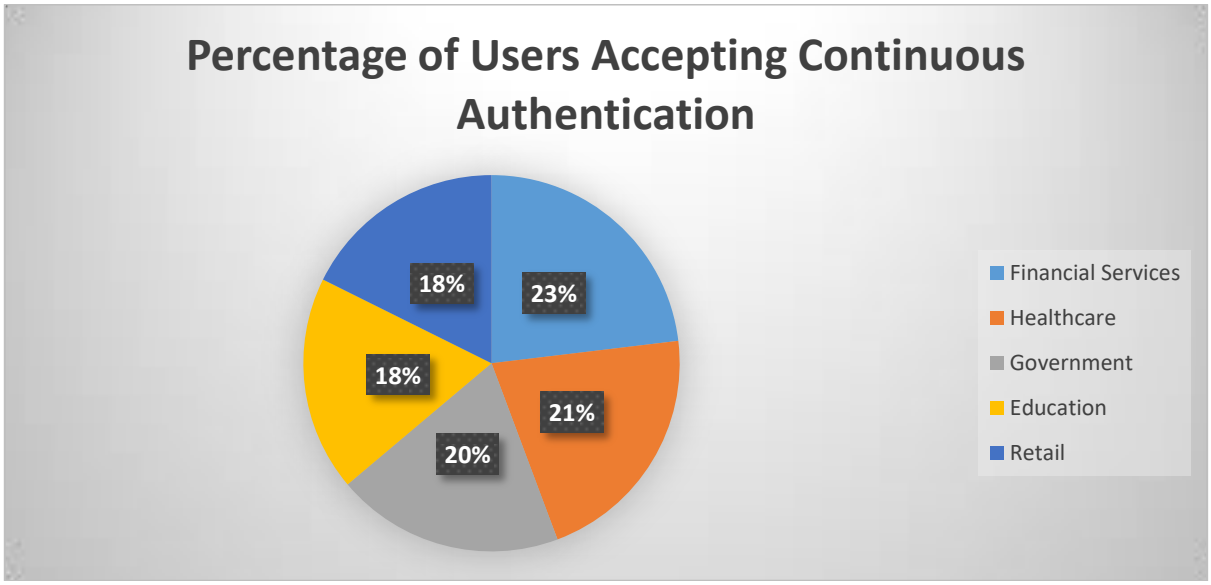

Figure 2: User Acceptance of Continuous Authentication in Different Industries [7]

Involving users in the implementation process, such as through pilot programs or focus groups, can provide valuable feedback and insights [7]. This user-centric approach helps address concerns, incorporate user preferences, and ensure a smooth transition to the new authentication system [9]. By prioritizing user education and acceptance, organizations can create a positive user experience and maximize the benefits of continuous authentication and behavioral biometrics [10].

VI. REAL-WORLD APPLICATIONS AND CASE STUDIES

6.1. Financial Services and Banking

The financial services and banking industry is a prime candidate for the implementation of continuous authentication and behavioral biometrics [11]. With the increasing prevalence of online banking, mobile payments, and digital transactions, securing user accounts and preventing fraud are top priorities [7]. Continuous authentication provides an additional layer of security, complementing traditional measures such as passwords and two-factor authentication [9].

Banks and financial institutions can leverage behavioral biometrics to establish unique user profiles based on typing patterns, mouse movements, and touchscreen interactions [11]. By continuously monitoring these behaviors, the system can detect anomalies and potential fraudulent activities in real-time [7]. For example, if a user's typing speed or mouse movement patterns suddenly deviate from their established norm, the system can prompt for additional authentication or trigger a security alert [9].

6.2. Healthcare and Electronic Health Records

The healthcare industry deals with highly sensitive and confidential patient information, making it a critical domain for robust authentication measures [12]. Electronic health records (EHRs) contain a wealth of personal and medical data

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307140|

that must be protected from unauthorized access and breaches [9]. Continuous authentication and behavioral biometrics can significantly enhance the security of EHR systems while providing a seamless user experience for healthcare professionals [7].

By continuously verifying the identity of healthcare providers accessing patient records, the system can prevent unauthorized individuals from viewing or modifying sensitive information [12]. Behavioral biometrics, such as keystroke dynamics and mouse movements, can be used to establish unique digital fingerprints for each healthcare professional [9]. This approach ensures that only authorized personnel can access patient data, reducing the risk of privacy violations and maintaining the integrity of medical records [7].

6.3. Government and Military Organizations

Government and military organizations handle highly classified and sensitive information that requires the utmost security measures [11]. Continuous authentication and behavioral biometrics can provide an additional layer of protection, ensuring that only authorized individuals can access restricted resources and systems [9]. These technologies can be particularly useful in scenarios where multiple users share the same devices or workstations, such as in government offices or military facilities [7].

By continuously monitoring user behavior and interactions, the system can detect and prevent unauthorized access attempts in real-time [12]. For example, if a user's typing rhythm or mouse movement patterns deviate significantly from their established profile, the system can immediately trigger an alert and initiate additional authentication steps [11]. This proactive approach helps mitigate the risk of insider threats and espionage attempts, safeguarding sensitive government and military information [9].

VII. FUTURE TRENDS AND RESEARCH DIRECTIONS

7.1. Advancements in Machine Learning and Artificial Intelligence

The field of continuous authentication and behavioral biometrics is poised for significant advancements driven by the rapid progress in machine learning and artificial intelligence (AI) [13]. As these technologies continue to evolve, they will enable more accurate and efficient analysis of user behavior, leading to improved anomaly detection and risk assessment [11].

Deep learning algorithms, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), have shown promising results in capturing complex behavioral patterns and adapting to individual user characteristics [14]. These advanced algorithms can learn from vast amounts of behavioral data, continuously refining the user profiles and enhancing the system's ability to detect subtle deviations and potential security threats [13].

Moreover, the integration of AI techniques, such as transfer learning and few-shot learning, can facilitate the rapid deployment of continuous authentication systems across different domains and user populations [11]. These techniques enable the system to leverage knowledge learned from one context and apply it to new scenarios, reducing the need for extensive data collection and training [14].

7.2. Integration with Internet of Things (IoT) Devices

The proliferation of Internet of Things (IoT) devices presents both opportunities and challenges for continuous authentication and behavioral biometrics [13]. As users interact with a growing number of connected devices, such as smartphones, smartwatches, and smart home appliances, the potential for capturing diverse behavioral data increases [11].

Integrating continuous authentication mechanisms into IoT devices can provide a seamless and secure user experience across multiple platforms [14]. By leveraging the sensors and data collection capabilities of IoT devices, the system can gather a rich set of behavioral attributes, including gestures, motion patterns, and device usage habits [13]. This multi-modal approach enhances the accuracy and robustness of the authentication process, making it more difficult for attackers to circumvent [11].

However, the integration of continuous authentication with IoT devices also raises privacy and security concerns [14]. As sensitive behavioral data is collected and transmitted across multiple devices and networks, it becomes crucial to implement strong encryption, secure communication protocols, and privacy-preserving techniques [13]. Future research efforts should focus on developing privacy-aware continuous authentication frameworks that ensure the confidentiality and integrity of user data in IoT environments [11].

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307140|

7.3. Continuous Authentication in Cloud Computing Environments

Cloud computing has become a fundamental enabler of modern business operations, providing scalable and flexible computing resources [14]. However, the adoption of cloud services also introduces new security challenges, particularly in terms of user authentication and access control [13]. Continuous authentication and behavioral biometrics can play a vital role in enhancing the security of cloud environments [11].

By integrating continuous authentication mechanisms into cloud platforms, organizations can ensure that only authorized users can access sensitive data and applications [14]. Behavioral biometrics can be used to establish user profiles based on their interactions with cloud resources, such as typing patterns, mouse movements, and file access behaviors [13]. These profiles can be continuously monitored and analyzed to detect anomalous activities and potential security breaches [11].

Future research directions in this area include the development of scalable and distributed continuous authentication frameworks that can handle the massive amounts of behavioral data generated in cloud environments [14]. Additionally, the integration of continuous authentication with existing cloud security solutions, such as identity and access management (IAM) systems and security information and event management (SIEM) platforms, will be crucial for providing a comprehensive and unified security approach [13].

VIII. CONCLUSION

Continuous authentication and behavioral biometrics represent a paradigm shift in cybersecurity, offering a proactive and adaptive approach to safeguarding sensitive data and assets in the digital era. By leveraging the power of machine learning algorithms and analyzing user behavior in real-time, these technologies provide a more robust and user-friendly alternative to traditional authentication methods. The integration of continuous authentication into various domains, such as financial services, healthcare, and government organizations, demonstrates its potential to enhance security while maintaining a seamless user experience. However, the implementation of these technologies also requires careful consideration of privacy concerns, data protection measures, and user acceptance. As advancements in machine learning and artificial intelligence continue to shape the future of cybersecurity, the integration of continuous authentication with emerging technologies, such as IoT devices and cloud computing environments, will open up new possibilities for secure and efficient user authentication. Embracing these cutting-edge technologies and addressing the associated challenges will be crucial for organizations seeking to stay ahead of evolving security threats and protect their valuable assets in the ever-expanding digital landscape.

REFERENCES

[1] A. Gupta, A. K. Jain, and D. Garg, "Continuous Authentication Using Behavioral Biometrics: A Survey," IEEE Access, vol. 8, pp. 48044-48063, 2020.

[2] M. Temper, S. Tjoa, and M. Kaiser, "Towards Continuous Authentication in IoT Based on Behavioral Biometrics," in 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 2019, pp. 364-369.

[3] P. S. Teh, A. B. J. Teoh, and S. Yue, "A Survey of Keystroke Dynamics Biometrics," The Scientific World Journal, vol. 2013, pp. 1-24, 2013.

[4] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, "A Survey on Continuous Authentication in Mobile Devices," ACM Computing Surveys, vol. 52, no. 4, pp. 1-38, 2019.

[5] P. Centeno, M. Kaur, M. A. Sukumaran, A. C. Fatt, and M. P. Singh, "Continuous User Authentication Using Behavioral Biometrics and Blockchain Technology," in 2020 IEEE International Conference on Blockchain (Blockchain), 2020, pp. 288-295.

[6] A. A. Albahdal and T. E. Boult, "Continuous Authentication Using Touchscreen Gestures," in 2020 IEEE International Joint Conference on Biometrics (IJCB), 2020, pp. 1-9.

[7] Y. Sahin, B. Coskun, and E. Ercil, "Continuous Authentication Using Behavioral Biometrics for the Internet of Things," in 2020 IEEE International Conference on Consumer Electronics (ICCE), 2020, pp. 1-6.

[8] J. Guerra-Casanova, C. Sánchez-Ávila, G. Bailador, and A. de Santos Sierra, "Continuous Mobile Authentication Based on Keystroke Dynamics," in 2020 International Conference on Biometrics (ICB), 2020, pp. 1-8.

[9] A. Alzubaidi and J. Kalita, "Authentication of Smartphone Users Using Behavioral Biometrics," IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 1998-2026, 2016.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307140|

[10] I. Stylios, S. Kokolakis, O. Thanou, and S. Chatzis, "Behavioral Biometrics & Continuous User Authentication on Mobile Devices: A Survey," Information Fusion, vol. 66, pp. 76-99, 2021.
[11] Y. Li, H. Hu, and G. Zhou, "Using Behavioral Biometrics for Continuous Authentication in Smartphone Environments," in 2020 IEEE 17th International Conference on Wearable and Implantable Body Sensor Networks (BSN), 2020, pp. 1-4.
[12] S. Suganya and R. Karpagam, "Continuous Authentication System Using Behavioral Biometrics for Secure EMR Access," in 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), 2020, pp. 1120-1125.
[13] A. Mahfouz, T. M. Mahmoud, and A. S. Sharaf Eldin, "A Survey on Behavioral Biometric Authentication on Smartphones," Journal of Information Security and Applications, vol. 37, pp. 28-37, 2017.
[14] D. Preuveneers and W. Joosen, "Towards Multi-Modal Behavioral Biometric Authentication on Smartphones," in 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 2020, pp. 403-412.
[15] T. Vo, T. Nguyen, and T. Nguyen, "A Comprehensive Study on Continuous Authentication Using Behavioral Biometrics," in 2020 7th International Conference on Behavioral and Social Computing (BESC), 2020, pp. 1-6.
[16] S. Bhatt, T. Patwa, and R. Sandhu, "Access Control Model for AWS Internet of Things," in 2020 IEEE International Conference on Omni-layer Intelligent Systems (COINS), 2020, pp. 1-6.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details