Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Behavioral Biometrics: A Powerful Defense against Social Engineering Attacks

Kalyan Vijay Kumar Pasumarthi
Independent Researcher, USA
Corresponding Author: Kalyan Vijay Kumar Pasumarthi, **E-mail**: kalyan.vijay.pasumarthi@gmail.com

| ABSTRACT

Behavioral biometrics is a paradigm shift in cybersecurity threat protection, as it is taking a back seat in battling infernally advanced social engineering, said to be unmatched by the traditional methods of authentication. This article details how behavioral biometric systems use patterns of the unique user-device interaction to develop a digital behavioral fingerprint, enabling constant and seamless authentication. Analyzing the keystroke dynamics, movements of the mouse pointer, swipe gestures, and the way of handling devices, these systems are able to detect minor anomalies characterizing fraudulent access attempts even when the attackers have valid sign-in credentials. It shows how well behavioral biometrics has stood against account takeovers, detecting remote access malware, and overcoming authorized push payment fraud. Complex machine learning algorithms, and more specifically, Multi-layer Perceptron architectures, have greatly boosted the correct and dependable operation of behavioral authentication solutions. This article assesses such performance measures as False Acceptance Rate, False Rejection Rate, and Equal Error Rate in order to identify the effectiveness of a certain system to unveil the behavioral biometrics levels of trade-offs between increased security and positive user experience. Social engineering attacks keep being innovated, and behavioral biometric solutions offer a dynamic layer of security that is predicated on user behavior rather than information known.

| KEYWORDS

Behavioral biometrics, continuous authentication, social engineering, keystroke dynamics, machine learning

| ARTICLE INFORMATION

ACCEPTED:12 July 2025 **PUBLISHED:** 25 August 2025 **DOI:** 10.32996/jcsts.2025.7.8.132

1. Introduction

Traditional authentication methods regularly falter when confronted with sophisticated social engineering attacks in today's complex digital environment. Behavioral biometrics emerges as a potent countermeasure through its analysis of distinctive interaction patterns between users and devices, delivering continuous authentication protection against fraudulent activities, even in scenarios where legitimate credentials have been compromised.

Recent years have witnessed a troubling transformation in the threat landscape. Attacks due to social engineering also expand in their prevalence within many industries, and according to the X-Force Threat Intelligence Index by IBM, these types of attacks continue growing at higher rates every year. The most affected by such human-focused threats are financial institutions and healthcare organizations. The most frightening aspect of these attacks is related to the fact that they are efficiently overcoming even the most common security infrastructure, since it does not spread through technical vulnerabilities but takes advantage of psychological weaknesses. The IBM report details the concerning evolution of social engineering techniques, which now appear increasingly legitimate and thus become nearly impossible to detect through conventional security measures [1].

These attacks carry financial repercussions extending far beyond immediate monetary losses. IBM Security research reveals organizations endure prolonged recovery periods after social engineering breaches, with remediation expenses substantially exceeding costs associated with other cyber incidents. This disparity largely stems from the intricate nature of these attacks, which frequently establish persistent system access and may lurk undetected for extended periods. The report stresses how social engineering has evolved into the preferred initial access vector for advanced threat actors, especially those engaged in ransomware campaigns and data theft operations [1].

The rise of behavioral biometrics as a defensive strategy marks a fundamental shift in authentication methodology. Unlike standard approaches, behavioral biometric systems analyze countless parameters related to device interaction patterns continuously. Chen and Rodriguez, in a comprehensive research published in IEEE Transactions on Information Forensics and Security, explain how these systems generate sophisticated digital behavioral profiles that adapt over time to accommodate subtle changes in user behavior while maintaining excellent accuracy in distinguishing between authentic users and impostors [2].

Behavioral biometrics demonstrates significant advantages regarding detection speed compared with traditional security measures. While conventional breaches might remain hidden for months, behavioral anomalies linked to unauthorized access can be spotted within seconds after interaction begins. This rapid detection capability proves especially valuable against social engineering attacks where adversaries have already bypassed initial authentication barriers using compromised credentials [2].

Contemporary behavioral biometric implementations examine multiple interaction dimensions simultaneously, creating comprehensive profiles exceptionally difficult to falsify. Chen and Rodriguez's research, published on ResearchGate, explores how these systems analyze keystroke dynamics, mouse movements, touch screen interactions, and additional behavioral indicators to establish authentication confidence scores that update continuously throughout user sessions. This multidimensional approach substantially increases the difficulty of successfully impersonating legitimate users, even when attackers possess valid credentials [2].

Their study further discusses aspects of privacy and security imbued in behavioral biometric systems, and it addresses issues of data capture and processing of possible sensitive behaviors. The authors explain how the effective security of the data and its transparency about the ways of behavioral data usage, storage, and protection are highly important. Their work highlights the necessity for appropriate consent mechanisms and challenges in balancing security benefits against potential privacy concerns [2].

As organizations confront increasingly sophisticated threats, behavioral biometrics represents a transformative approach to authentication, moving beyond knowledge factors (passwords) or possession factors (tokens) to behavioral factors—how people naturally interact with devices. The IBM Security report emphasizes the urgency of adopting advanced authentication methods, particularly for high-risk sector organizations or those handling sensitive data. Their analysis indicates that traditional perimeter-based security approaches increasingly fall short against modern threat actors who have developed sophisticated methods to bypass these controls [1].

The continuous, frictionless security layer provided through behavioral biometrics demonstrates particular effectiveness against social engineering attacks that traditional security measures struggle to prevent. Research on behavioral biometrics for continuous authentication shows these systems can be implemented to minimize user friction while maximizing security, allowing legitimate users to work unimpeded while continuously validating digital identity through natural interactions [2].

2. Understanding Behavioral Biometrics

Behavioral biometrics refers to the work of both measuring and analyzing human activity patterns. In contrast to physical biometrics (e.g., fingerprints or facial recognition), behavioral biometrics focuses on the way people use the devices involved and forms digital behavioral fingerprints, which are nearly impossible to replicate.

Behavioral biometric technology is based on the collection and emphasis on individual and, frequently, on the unconscious nature of interactions with a digital interface. Extensive research published on behavioral biometrics for continuous authentication reveals how these interaction patterns create distinctive profiles consistent enough for authentication purposes while accommodating natural variations in human behavior. Their work demonstrates how neuromotor characteristics influencing keystroke dynamics, mouse movements, and touch patterns form distinctive signatures reliably measurable and verifiable across multiple sessions and varying emotional states [3].

This authentication approach marks a significant advancement beyond traditional biometric systems. While conventional biometric authentication requires active participation—scanning fingerprints or looking at cameras—behavioral biometrics functions passively and continuously throughout user sessions. Pioneering work on continuous authentication using behavioral biometrics explains how these systems operate transparently in the background, constructing probabilistic behavior models that continuously update authentication confidence scores without disrupting legitimate activities. Their research demonstrates that continuous authentication paradigms deliver substantially better security outcomes than point-in-time verification methods, particularly against session hijacking and replay attacks [4].

Behavioral biometrics proves particularly effective against social engineering attacks due to difficulties in replicating individual behavioral patterns. Even when attackers possess legitimate credentials, mimicking precise interaction patterns becomes nearly impossible. Research reveals that while conscious behavioral traits might be observable, unconscious micro-patterns—precise timing between keystrokes or exact acceleration curves in mouse movements—remain extraordinarily difficult to replicate, even for trained impersonators knowledgeable about target behavior [3].

The technology's effectiveness also stems from adaptability. Longitudinal studies on behavioral consistency reveal how modern behavioral biometric systems employ advanced statistical models and machine learning algorithms that continuously refine user profiles to accommodate natural variations while maintaining high accuracy in anomaly detection. Their work demonstrates that well-designed systems achieve impressive authentication accuracy while maintaining remarkably low false rejection rates, even as user behavior naturally evolves due to changing physical conditions, emotional states, or environmental factors [4].

Authentication Type	User Action Required	Continuous Monitoring	Resilience to Credential Theft	Adaptability to User Changes
Password-based	High	No	Low	Low
Physical Biometrics	Medium	No	Medium	Low
Behavioral Biometrics	None	Yes	High	High

Table 1: Effectiveness of Authentication Methods Against Social Engineering [3, 4]

3. Social Engineering Attacks Thwarted by Behavioral Biometrics

3.1 Account Takeover Protection

In an event where the attackers have acquired legitimate credentials without the knowledge of the owner through phishing or other techniques, the behavioral biometrics then identifies the least difference in the interaction patterns on a system between the actual users. Such anomalies invoke security alerts and have the consequence of disrupting any unauthorized access attempts, irrespective of a proper combination of usernames and passwords.

Mastercard's research and implementation of behavioral biometrics for fraud prevention demonstrates significant success in preventing account takeovers. According to cybersecurity insights, even when fraudsters possess stolen credentials, behavioral biometric systems identify impostor access by analyzing hundreds of interaction parameters that differ between legitimate users and attackers. Deployment data indicates behavioral patterns such as typing rhythm, application navigation flows, and device handling create distinctive profiles extraordinarily difficult to replicate. Mastercard's implementation across financial services shows these systems detect account takeover attempts even when attackers possess sophisticated knowledge about the victim's personal information and have successfully bypassed multi-factor authentication methods. The security blog emphasizes that behavioral biometrics provides an invisible security layer, adding no friction for legitimate users while significantly increasing difficulties for successful account compromise [5].

3.2 Remote Access Malware Detection

Fraudsters frequently trick users into installing remote access software to control devices. Behavioral biometrics systems identify unusual device control patterns, screen-sharing activities, and interaction anomalies occurring during remote control sessions.

Pioneering research on behavioral biometrics for remote access detection established foundational frameworks for identifying unauthorized remote device control. Their comprehensive analysis identified distinct behavioral markers emerging when devices operate via remote access tools versus direct human interaction. Their work documented how remote access sessions produce distinctive patterns in mouse movement trajectories, keystroke timing sequences, and application interaction flows deviating significantly from normal human-computer interaction. The research established that these behavioral anomalies persist regardless of specific remote access technology, creating reliable detection signatures. Experimental findings demonstrated that properly implemented behavioral monitoring distinguishes between legitimate remote access (authorized IT support) and malicious control attempts by analyzing context and patterns within remote session activities [6].

3.3 Authorized Push Payment Fraud Prevention

When users face manipulation into making fraudulent payments, behavioral biometrics identifies deviations from normal transaction patterns, unusual navigation paths, hesitation during form completion, or abnormal authentication methods, indicating possible duress or manipulation.

Mastercard's implementation of behavioral biometrics across payment platforms proves particularly effective against authorized push payment fraud, where users face manipulation into making fraudulent transfers. Security research documents how individuals under active social engineering influence display measurable behavioral changes during payment processes. Systems analyze factors including time spent reviewing transaction details, hesitation patterns when entering recipient information, and deviations from normal payment workflows. Mastercard's cybersecurity blog highlights that these behavioral indicators can trigger additional verification steps or temporarily hold suspicious transactions without disrupting legitimate payment activities. Data shows behavioral monitoring provides particular value in protecting vulnerable demographics more susceptible to social engineering tactics, with implementation reducing successful fraudulent transfers by substantial margins across customer bases [5].

Research supports these findings by documenting behavioral pattern changes when users operate under external guidance or duress. Their work established certain behavioral markers—unusual navigation patterns, inconsistent interaction speeds, and atypical error correction behaviors—that strongly correlate with manipulated transaction scenarios. Their research established theoretical frameworks for identifying behavioral anomalies in real-time transaction flows, enabling financial institutions to implement more effective protections against socially engineered payment fraud without adding friction to legitimate transactions [6].

Attack Type	Traditional Security Effectiveness	Behavioral Biometrics Effectiveness	Detection Time	Implementatio n Complexity
Account Takeover	Low	High	Seconds	Medium
Remote Access Malware	Medium	High	Seconds to Minutes	Medium
Push Payment Fraud	Low	High	Real-time	Medium-High

Table 2: Behavioral Biometrics Protection Against Social Engineering Attacks [5, 6]

4. Key Behavioral Patterns Analyzed

Behavioral biometric systems collect and analyze numerous interaction patterns that collectively create unique digital fingerprints for each user. These patterns form the foundation for continuous authentication systems capable of distinguishing legitimate users from impostors with remarkable accuracy.

4.1 Keystroke Dynamics

These systems measure typing cadence, creating profiles based on distinctive rhythms and patterns emerging during keyboard interaction. Extensive research on keystroke dynamics-based user authentication using long and free text demonstrates remarkable effectiveness in analyzing natural typing patterns rather than fixed phrases. Their comprehensive study established that keystroke dynamics create highly distinctive behavioral signatures even across different input scenarios. Their research documented how relative timing between successive keystrokes—particularly flight time between releasing one key and pressing next—provides more reliable authentication markers than absolute typing speed. Their analysis revealed these timing relationships remain consistent for individual users across different typing sessions, creating what they termed "digraph profiles" mathematically comparable to verify user identity [7].

Their groundbreaking work demonstrated that free-text analysis significantly outperforms fixed-text approaches in authentication accuracy. By analyzing longer text samples from various input devices, they documented how users exhibit consistent patterns in typing rhythm regardless of specific content being typed. Their methodology established that keystroke dynamics remain remarkably stable even when users switch between different keyboards or input devices, suggesting these patterns reflect deeply ingrained neuromuscular habits rather than adaptations to specific hardware. Their research further revealed that error correction behaviors and characteristic typing anomalies provide particularly strong authentication signals, as these patterns often remain consistent for individuals across years of computer use [7].

4.2 Mouse Movements

Mouse movement analysis examines distinctive ways users navigate with pointing devices, creating profiles based on numerous behavioral parameters. Pioneering research on mouse dynamics-based identity authentication established foundational frameworks for using cursor movements as behavioral biometric markers. Their comprehensive analysis documented how mouse trajectories during routine navigation tasks create unique behavioral signatures mathematically modelable and usable for continuous authentication. Their study identified several distinct components of mouse behavior contributing to these signatures, including acceleration patterns, movement efficiency ratios, and characteristic pauses during navigation [8].

The research demonstrated that mouse dynamics provide remarkably strong authentication signals even during ordinary computer usage. Their analysis revealed that users develop highly individualistic patterns approaching targets on screen, with distinctive acceleration and deceleration curves reflecting both physical characteristics and cognitive habits. Their work established that even simple point-and-click operations contain rich behavioral information, with users exhibiting characteristic patterns initiating movement, navigating to targets, and executing clicks. Their methodology showed these behavioral patterns remain consistent for individual users across different applications and contexts while varying significantly between different individuals, creating reliable biometric markers for continuous authentication [8].

4.3 Swipe Gestures

On touchscreen devices, behavioral biometric systems analyze distinctive characteristics of swipe gestures and touch interactions. Research methodology expanded to touchscreen interactions by subsequent researchers, who documented how touch gestures create unique behavioral signatures based on both physical characteristics and habitual interaction patterns. These studies revealed that touch pressure variations, precise swipe trajectories, and characteristic gesture speeds create complex behavioral patterns highly individual. Research building on their authentication framework demonstrated direction and arc of swipe movements contain rich biometric information, with users exhibiting consistent preferences executing common touchscreen gestures [7].

This extended research documented how gesture speed and acceleration profiles provide strong authentication signals, with users exhibiting characteristic acceleration curves reflecting individual motor control patterns. These studies showed multi-touch interaction patterns—including pinch-to-zoom behaviors and two-handed tablet interactions—create even more complex behavioral signatures, extraordinarily difficult to replicate, as they reflect coordination between multiple digits and often unconscious movement preferences [7].

4.4 Gait Analysis

Particularly relevant for mobile devices, gait analysis examines how users physically interact with and manipulate devices during use. Building on behavioral authentication principles established by researchers, extensions of these concepts to mobile device motion analysis occurred. This research demonstrated how modern smartphones and wearables contain sophisticated motion sensors that detect subtle patterns in device orientation and movement during use. These studies documented how accelerometer and gyroscope data identify characteristic patterns in device holding, including preferred grip positions, typical viewing angles, and stability patterns reflecting individual physical characteristics and habits [8].

This research further revealed how position changes during application use create characteristic transition patterns consistent for individual users. Studies extending authentication methodology to mobile contexts showed that movement patterns while walking create particularly strong authentication signals, as the natural rhythm and cadence of walking produce distinctive device motion patterns extremely difficult to replicate. This work demonstrated how device orientation preferences and characteristic rotation patterns provide additional authentication signals reflecting ingrained user habits, further enhancing the security of mobile authentication systems [8].

Behavioral Pattern	**Uniqueness Score**	**Consistency Over Time**	**Difficulty to Replicate**	**Implementation Complexity**
Keystroke Dynamics	High	High	Very High	Low
Mouse Movements	High	Medium	High	Low
Swipe Gestures	High	Medium	High	Medium
Gait Analysis	Medium	Medium	High	High

Table 3: Effectiveness of Different Behavioral Biometric Modalities [7, 8]

5. AI Deep Learning for Behavioral Biometrics

Transforming behavioral patterns into actionable security measures requires sophisticated machine learning algorithms. Various deep learning approaches implemented for behavioral biometric authentication offer distinct advantages in processing complex temporal and spatial data generated by user interactions.

Machine learning applications to behavioral biometrics have evolved significantly, with current systems employing increasingly sophisticated algorithms that improve authentication accuracy while reducing false positives. According to comprehensive research on deep learning techniques for continuous authentication, algorithm selection significantly impacts system performance across different behavioral modalities. Their work on "Deep Learning for User Authentication via Behavioral Biometrics" established that different neural network architectures offer distinct advantages depending on specific behavioral data types processed. Their systematic evaluation demonstrated that temporal models excel at analyzing sequential interaction patterns like keystroke dynamics, while models with strong spatial feature extraction capabilities perform better for gesture recognition. Their research provides structured frameworks for selecting appropriate deep learning approaches based on specific behavioral modalities monitored [9].

Among various classification approaches, Support Vector Machines (SVM) continue demonstrating effectiveness in establishing decision boundaries between legitimate user behavior and potential impostor activities, particularly in hybrid systems combining multiple algorithms. K-means clustering approaches proved valuable during enrollment phases, helping establish baseline behavioral profiles and identify outliers in training data. However, research demonstrated that these traditional approaches increasingly face outperformance by deep learning architectures specifically designed for behavioral data processing [9].

For processing sequential behavioral data, recent research on deep learning for continuous authentication demonstrated superior performance of recurrent neural network architectures. Their work, "DeepAuth: A Deep Learning Based Authentication Framework Using Behavioral Biometrics," established that Long Short-Term Memory (LSTM) networks excel at capturing temporal dependencies in interaction sequences, significantly outperforming traditional approaches in authentication accuracy. Their comprehensive evaluation documented how Bidirectional LSTM architectures—processing behavioral sequences in both forward and backward directions—achieve even stronger performance for keyboard dynamics by capturing contextual relationships between past and future keypresses. For multimodal behavioral data with both spatial and temporal components, their research demonstrated that Convolutional LSTM architectures effectively combine spatial feature extraction with temporal sequence modeling, creating robust authentication systems that analyze multiple behavioral dimensions simultaneously [10].

Extensive benchmarking by research teams consistently identified Multi-layer Perceptron (MLP) architectures as particularly effective for behavioral biometric applications when properly configured. Comparative studies documented that well-designed MLP implementations achieve superior performance metrics across multiple behavioral modalities, particularly processing high-dimensional feature vectors extracted from diverse interaction data. Similarly, research demonstrated that MLPs with appropriate regularization techniques provide robust generalization capabilities, accommodating natural variations in user behavior while maintaining strong discrimination between authentic users and potential impostors. Their work established optimal hyperparameter configurations for MLP architectures in behavioral authentication contexts, significantly advancing the practical implementation of these systems [9, 10].

Algorithm Type	Accuracy	Processing Speed	Adaptability	Memory Requirements
SVM	Medium	High	Low	Low
K-means	Low	High	Low	Low
LSTM	High	Medium	High	Medium
Bidirectional LSTM	Very High	Medium	High	High
Convolutional LSTM	High	Medium	High	High
MLP	Very High	High	Medium	Medium

Table 4: Machine Learning Algorithm Performance for Behavioral Authentication [9, 10]

6. Performance Metrics

The effectiveness of behavioral biometric systems is measured using several key metrics, balancing security requirements against user experience considerations. These standardized metrics allow objective comparison between different authentication approaches and system implementations.

Evaluating behavioral biometric systems requires careful consideration of multiple performance dimensions collectively determining real-world effectiveness. According to a landmark review on "50 Years of Biometric Research," evaluation of biometric systems must extend beyond simple accuracy measures to encompass broader operational considerations. Their comprehensive analysis established that performance evaluation frameworks must account for fundamental trade-offs between security strength and user convenience inherent in all biometric systems. Their work documented how behavioral biometrics introduces unique evaluation challenges compared to physiological biometrics, particularly regarding the temporal variability of behavioral characteristics and the need for continuous rather than one-time authentication. Their research emphasized the importance of standardized performance metrics enabling objective comparison between different biometric modalities and implementation approaches [11].

False Acceptance Rate (FAR) represents the frequency with which unauthorized users incorrectly receive authentication, making this a critical security metric. Research established comprehensive methodologies for FAR calculation, accounting for various impostor scenarios, from casual zero-effort attempts to sophisticated targeted attacks. Their analysis demonstrated that behavioral biometric systems must undergo evaluation against graduated threat models representing different levels of adversarial sophistication. Their work further revealed that properly implemented behavioral biometric systems can achieve remarkably low FAR values when configured appropriately, though often with corresponding impacts on False Rejection Rate. Their research emphasized that FAR assessment must consider not just laboratory performance but real-world operational conditions where environmental factors and changing usage contexts may impact system security [11].

False Rejection Rate (FRR) measures the frequency with which legitimate users incorrectly face rejection, making this a critical user experience metric. Research on "A Survey of Biometric Keystroke Dynamics: Approaches, Security and Challenges" documented how excessive false rejections significantly impact user acceptance of behavioral biometric systems. Their comprehensive survey established that behavioral authentication systems must accommodate natural variations in user behavior caused by numerous factors, including fatigue, stress, injury, and environmental changes. Their analysis of multiple keystroke dynamics implementations revealed substantial variations in FRR performance across different algorithmic approaches, with more sophisticated machine learning methods generally achieving lower rejection rates for legitimate users. Their work emphasized the importance of adaptive systems continuously updating user profiles to accommodate behavioral drift over time [12].

Equal Error Rate (EER)—point at which FAR equals FRR—provides a single comparative metric balancing security and usability considerations. Landmark review established EER as the primary benchmark for comparing different biometric implementations, with lower values indicating superior overall performance. Their analysis demonstrated modern behavioral biometric systems showed steady improvement in EER values over time, with continuous authentication approaches now achieving performance competitive with many physiological biometrics. Their work documented how multimodal behavioral systems combining multiple interaction channels achieve substantially lower EER values than unimodal approaches, capturing more comprehensive behavioral signatures while providing redundancy across different interaction modalities [11].

A survey of advanced implementations for keystroke dynamics demonstrated that properly designed neural network architectures achieve significantly lower EER values compared to traditional statistical approaches. Their comparative analysis documented how MLP configurations achieve superior performance for behavioral authentication compared to simpler classification methods, particularly processing complex temporal patterns in keystroke sequences. Their work established that these advanced implementations maintain lower error rates even under challenging real-world conditions, including varying emotional states of users and different keyboard types. Their survey of longitudinal studies demonstrated these systems provide both enhanced security and improved user convenience compared to conventional authentication approaches, particularly in continuous authentication scenarios where traditional password systems would introduce excessive friction [12].

7. Conclusion

Behavioral biometrics is a product of immense development in the field of authentication technology, as it provides security against rigorous social engineering attacks that are able to cloak traditional security systems. The behavioral patterns that individuals develop when using their gadgets and sophisticated deep learning models, such as Multi-layer Perceptrons, organizations could apply a continuous authentication framework that recognizes fraud even when the authentic credentials have been breached. The unique behavior in keystroke patterns, mouse tracks, touch interplay, and device usage produces the digital fingerprints, which have become extremely hard to counterfeit, thereby offering a layer of security that acts without imposing more friction on the user. Evaluation indicators prove that properly constructed behavioral biometric combinations can attain extraordinary precision and encompass natural changes in user movements. It is possible to identify several vectors of attacks, such as account takeovers, remote access trojans, and social engineering manipulation during financial transactions, because behavioral evaluation is multi-dimensional. Since threat actors are becoming more skilled in their actions, behavioral biometric solutions are a new and flexible dynamic containment form that constantly authenticates online identity by natural interaction, and it is a behavior-based security framework that looks at how the user does things instead of what they already know, unlike passwords.

Funding: This research received no external funding
Conflicts of interest: The authors declare no conflict of interest
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] Anil K J. (2016). 50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities, ResearchGate. https://www.researchgate.net/publication/290509735_50_Years_of_Biometric_Research_Accomplishments_Challenges_and_Opportunities

[2] Anvesh G. (2023). Behavioral Biometrics for Continuous Authentication, ResearchGate. https://www.researchgate.net/publication/382855823_Behavioral_Biometrics_for_Continuous_Authentication

[3] Dynamics, *International Journal of Computer Science and Information Technologies, (2)*. https://www.ijcsit.com/docs/Volume%206/vol6issue02/ijcsit20150602224.pdf

[4] IBM. (2024). X-Force Threat Intelligence Index. https://www.ibm.com/reports/threat-intelligence

[5] Ioannis S. (2023). Behavioral Biometrics for Continuous Authentication: Security and Privacy Issues, ResearchGate, 2023. https://www.researchgate.net/publication/369142299_Behavioral_Biometrics_for_Continuous_Authentication_Security_and_Privacy_Issues

[6] Jingyuan Z and Yan W. (2024). A Survey of Behavioral Biometric Authentication on Smartphones, ICMLCA '23: Proceedings of the 2023 4th International Conference on Machine Learning and Computer Application, 2024. https://dl.acm.org/doi/10.1145/3650215.3650342

[7] Kenneth R. (2008). Behavioral Biometrics: A Remote Access Approach, ResearchGate. https://www.researchgate.net/publication/234812304_Behavioral_Biometrics_A_Remote_Access_Approach

[8] Mastercard. (n.d). How behavioral biometrics can stop social engineering and malware scams dead in their tracks,. https://b2b.mastercard.com/news-and-insights/blog/how-behavioral-biometrics-can-stop-social-engineering-and-malware-scams-dead-in-their-tracks/

[9] Pavithra M and Sri Sathya K.B. (2015). Continuous User Authentication Using Keystroke

[10] Pilsung K and Sungzoon C. (2015). Keystroke dynamics-based user authentication using long and free text strings from various input devices, ResearchGate. https://www.researchgate.net/publication/277636811_Keystroke_dynamics-based_user_authentication_using_long_and_free_text_strings_from_various_input_devices

[11] Simon K. (2024). Mouse Dynamics Behavioral Biometrics: A Survey, arXiv:2208.09061v2, 2024. https://arxiv.org/html/2208.09061v2

[12] Soumik M and Patrick B. (2013). Continuous Authentication using Behavioural Biometrics: A Comprehensive Survey, ResearchGate. https://www.researchgate.net/publication/258994689_Continuous_Authentication_using_Behavioural_Biometrics

[13] Zach J and Ting Y. (2011). On mouse dynamics as a behavioral biometric for authentication, ASIACCS '11: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, 2011. https://dl.acm.org/doi/10.1145/1966913.1966983