International Journal of Research in Science and Technology

Volume 13, Issue 01: January-March 2026

ISSN 2394 - 9554

Behavioral-Based Authentication for Business Accounts Using Hidden Markov Models on Mouse Movement Data

Roberto Acevedo Facultad de Ingeniería, Universidad San Sebastián, Bellavista 7, 8420524, Santiago, Chile.

roberto.acevedo.llanos@gmail.com

Abstract

One new technique that is coming up is behavioral-based authentication where users can be identified by their specific behavioral patterns which here include the movements of the mouse. This paper concentrates on the vision of using Hidden Markov Models (HMM) to study the behavior of the mouse to know how to get business accounts. Common authentication systems such as passwords and tokens can be stolen, phished, and re-played. Biometric systems, more secure though capable of being spoofed, are not able to authenticate users continuously as they are in active sessions. In order to overcome these constraints, we introduce a new model known as Mouse Behavior Authentication with HMM (MBA-HMM) which takes advantage of the statistical strength of the HMM to model and identify the actual user behavior using mouse trajectory data. The model includes pre-processing raw information on mouse movements, deriving both temporal and spatial information, and learning user-specific HMMs to identify abnormalities in real-time. To detect genuine users and non-genuine users in business applications, MBA-HMM is constantly tracking the patterns of mouse movement. It is a passive and unobtrusive agent that works in the background and improves the security without interfering with the user experience. The experimental and testing of the proposed method on actual mouse movement data reveals that it has a promising future. MBA-HMM performed well in user identification and resisted imitation attacks as well as false acceptance and rejection. These results indicate how effectively behavioral biometrics, specifically, mouse dynamics based on HMMs can be used as a strong solution to the need to improve the security of business account authentication systems.

Keywords: *Behavioral-based authentication, HMM, mouse movement data, user behavior modeling, continuous authentication, etc.*

1. INTRODUCTION

Background on behavioral biometrics and their role in cybersecurity

With the rising rate and complexity of attacks over the past few years, there is, by all means, a need to improve cybersecurity solutions [1]. Traditional authentication systems based on passwords, PIN or physical tokens are easily phished, forced down by brute force and credential theft victims. Even though the concept of multi factor authentication is more secure in nature, it can be complex at times and susceptible to some forms of social engineering and repetitive attacks [13]. As a possible solution to these issues in the modern security system, behavioral biometrics has evolved [2].

Behavioral biometrics: This is the method of identifying and verifying people based on their unique behavioral patterns in their interaction with the tools [3] [4]. Behavioral biometrics research dynamic and difficult to duplicate and ever-present traits as opposed to physiological biometrics (e.g. fingerprints or face recognition). Some of them include mouse movements, keyboard playing, walking, touch screen movements. The only advantage with behavioral biometrics is that they can offer both continuous

https://doi.org/10.64151/PSGCARE-20

ISSN 2394 - 9554

authentication, thus authenticating a user not only at login, but also throughout the entire session without impacting user experience[14].

Behavioral biometrics is an aspect of security systems that provides a real-time, non-invasive protection. It can be used to indicate something suspicious suggesting that the assailant has unlawful access even in situations where the attacker has valid credentials [5]. Behavioral patterns are hard to precisely copy, so with time machine learning models can adapt to even minor alterations in the actual-world behavior, thus better reinforcing these systems to the changing threats. Behavioral-based systems are also quite compatible with the concept of zero-trust architecture, where the actor or action is not trusted in any particular manner [15]. It is also the case that constant behavior enables systems to mix usability and protection efficiently, and therefore maintain security without causing the user unnecessary pain. Because of these advantages, in particular, in such areas like banking, corporate IT and healthcare where the security of constant access is of paramount importance, behavioral biometrics has been rapidly gaining popularity.

Importance of securing business accounts

Business data, finances as well as access to critical internal systems are laden to business accounts. Unauthorized access to such accounts may have legal consequences, data leaks, loss of money, and reputation damage among others. Given the fact that companies are increasingly relying on the digital technology and remote working conditions, it becomes more challenging to establish secure access control. Traditional approaches of account security are not enough. Smarter, dynamic and endless authentication systems that are capable of mitigating all internal risks as well as external attackers without halting throughout output are highly desired.

Overview of mouse movement as a behavioral trait

The character of interaction that a graphical interface offers to a user is reflected in movement behavior of a mouse. Speed, direction switches, patterns of clicks, pauses, angles of the trajectory, all of this might be useful to represent the slight but consistent activity. Another good behavioral biometric that can be used in user identification is mouse dynamics because these characteristics are hard to intentionally duplicate. Furthermore, mouse action is evolving naturally as people use computers hence permitting continuous and unnoticeable data gathering. The analysis of the mouse movements is therefore rather significant to desktop computers in companies where frequent authentication without user interruption is necessary.

Motivation for using Hidden Markov Models

Hidden Markov Models (HMMs) are ideal in predicting data sequencing with time-dependencies, and this is why it was fitted to track the patterns of mouse movement over time. They are able to recognize true versus pathological sessions and learn probabilistic state transitions of user behavior dynamics. HMMs are an excellent way of detecting minor changes in behavioral data due to their statistical sensitivity and adaptability, enabling to guarantee consistent continuous authentication.

Outline of the paper

In this paper, the relevant work is discussed as well as a proposed MBA-HMM model, experimental design and data, analysis of performance results, and practical applications. The findings are highlighted in the second section as well as suggestions of how behavior-based authentication systems should be developed further.

https://doi.org/10.64151/PSGCARE-20

ISSN 2394 - 9554

2. Related Work

Behavioral biometrics such as voice, motion, and dynamics of the keyboard have unique and consistent user identification solutions. This paper is exploring innovative methods especially to maintain constant user validation that enhances security in corporate accounts, and also deals with the incorporation of behavioral data with artificial intelligence.

Privacy-Preserving Behavioral Anonymization (PPBA)

The work would anonymize behavioural biometric data, including speech, movement, hand gestures, eyegaze, heartbeat (ECG) and brain activity (EEG), so as to uphold the privacy of a person[7]. Systematically discussing the existing anonymizing methods, the study categorizes them based on operational policies, privacy goals, advantages and disadvantages. It highlights that certain forms of liking speech have attracted so much attention but others such as the eye-gaze and brain activity are still under researches. Research on the ways of anonymizing behavior suggests that there is a certain need to enhance the process to ensure that privacy is protected appropriately when managing personal information on behavior.

Session-Replay Bot Detection System (SRBDS)

This dissertation is especially interested in advanced internet bots, namely, session-replay bots, which are able to recreate human behavior to impersonate humans [16]. The paper is dedicated to attacks of these bots on websites such as news, banking and gambling where such behavior is exhibited by the users. To replicate these assaults, the researcher created a prototype session-replay bot (ReBot) adding randomization to assess evasiveness. The work proposes the use of deep learning techniques for bot detection and randomization of websites as a moving-target defensive system to prevent bot attacks. Additionally considered for proactive protection are generative models for automated bot session construction.

RL-Based Continuous Keystroke Authentication (RLCKA)

This paper introduces a dynamic keyboard-based continuous authentication method utilizing reinforcement learning (RL) for authentication of users [8]. Enduring supervision of the user by the technology enhances traditional session authentication. The RL model is trained to find anomalies in typing behavior and flag suspicious activity[9]. The model is trained to identify patterns of changes over time using the double deep Q-network (DDQN) algorithm and the principal component analysis (PCA). Assessment results of widening data handling indicate that the system performs with satisfactory accuracy and minimal equal error rate (EER), thus enhancing its authentication ability.

Enhanced Behavioral Privacy Anonymization (EBPA)

Personal privacy protection in control of behavioral biometric data such as speech, gait, eye-gaze, and brain activity is researched in this work. Reviewing existing anonymizing techniques for these characteristics, the research categorizes them based on their privacy goals, conceptual significance, advantages and limitations[17]. The findings of the research are that despite the fact that certain features such as eye-gaze and brain activity have not been researched extensively compared to the highly researched ones, there has been research on them. It further suggests that more effective behavioral anonymizing tools may be justified by more effective assessment techniques.

This study examines new methods of authentication using behavioral biometrics voice, motion, and keyboard dynamics. It puts a strong emphasis on privacy protection, security improvements, and future

https://doi.org/10.64151/PSGCARE-20

advancements in continuous authentication solutions both in corporate settings and continuous, non-invasive user verification based on artificial intelligence-driven models [10].

Problem Statement and Challenges

Security gaps in existing authentication mechanisms

Despite their role as the first line of defense, there are numerous weaknesses to the passwords/OTPs, biometric scans that are available. OTPs may be lined with phishing, stolen, guessed or shared. Though more secure, even biometric may be cheated with high-quality reproduction or photographs. After an attacker has got in, in most cases there is no system that keeps track of the authenticity of a session that is undergoing. Insider threats, session issues and unlawful access find their way into commercial systems through these security weaknesses. Most of these techniques are not flexible also and are not able to identify behavioral deviations once access is gained. This requires a transition to smart authentication which is operational during the entire user session and which reacts to suspected actions in real time.

Issues with static and one-time authentication methods

Typically, when a user logs in, the identity of the user is merely identified once by using the static authentication mechanism. This method also assumes, which is not frequently true, that the valid user is also authorized user throughout the session. In case of credentials breach or a session hijacking at the time of a log-in, the system does not have measures of identifying malevolent activity. Additionally poor in flexibility of behavior as time or context goes by that is, remote access vs in-office access are they single measures. This leaves blind spots in the dynamic business world where malicious other players might pass unnoticed. In addition failure to distinguish between authorized users and imposters who duplicate themselves after authenticating are stationary systems which points to the extreme importance of authenticating user identity on a regular and explicit basis.

Need for continuous, non-intrusive, and user-specific methods

To adequately solve the problem of cybersecurity of the present day, contemporary authentication has to evolve to become uniform, flexible, and personalized. There is constant authentication of users to verify them during the entire session as well as during login. Nevertheless, these solutions should be non-invasive in the case that they can be utilized and manufactured. This involves the utilization of the naturally occurring user behavior that is of mouse movements that does not require the user to work harder. Since it is unique and hard to duplicate, it means that behavioral biometrics can offer custom security profiles, which can change over time. Such strategies are usually helpful in a corporate environment, where employee conduct can be insidiously monitored without causing disruption to the operations of the company. Continuous, behavior-based system is needed to maintain enjoyment and efficiency of the users and provide more solid security.

Proposed Framework: MBA-HMM

Introduction to the proposed method

MBA-HMM is an authentication method that is behaviour based, and was created to defend corporate accounts. It establishes the identity of the constantly users and passively monitors the movement pattern of the users in the use of the system in its normal operations. The architecture provides an extensible, non-invasive means of attempting to remove the drawbacks of static and intrusive approaches. MBA-HMM tries to build features of idiosyncratic behavior in mouse movements and creates personalized models that could detect anomaly, which is one of the signatures of unauthorized entry. This will ensure

https://doi.org/10.64151/PSGCARE-20

ISSN 2394 - 9554

that certain suspicious activities in the session can raise alarm or the access is shut off instantly in case of hijacked login passwords.

Overview of the system architecture

Training and verification are part of the MBA-HMM system to a large extent. The data of the mouse movement of authenticated users is collected and used in training using Hidden Markov Models to obtain individual behavior models. By gathering mouse real-time data during authentication, they are compared with these models and whether to identify a user or not decided. Throughout the acquisition of data, preprocessing, extraction of features, training of HMM to real-time evaluation and decision making, the architecture is filled with modules in each. Everything is happening in the background without making noise hence no interference. Scalable deployment into many user environments is achieved and the established business systems are easily interacted with because of its modular nature.

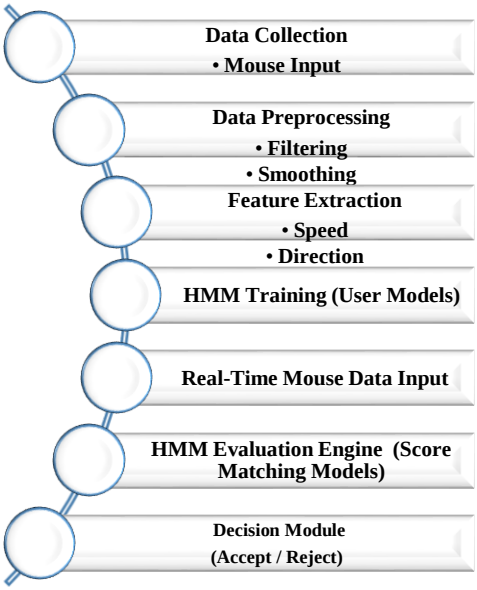

Fig 1: MBA-HMM System Architecture

Data collection and preprocessing

The movement of the mouse is data generated by the regular user activity and does not involve specific tasks or user instructions. This information consists of clicks, motions, timestamps and cursor locations among others. Preprocessing is characterized by the division of the information into the consumable sessions, scaling the coordinates according to the screen size, and filtering the raw data to eliminate noise and outliers. Periods of jitter caused by hardware are filtered out, as well as any sudden jumps[11]. This measure will guarantee the research is restricted to interesting and similar patterns of movement. To have good behavioral models that have the ability to accurately represent user behavior and identify anomalies, good preprocessing is required.

$$2q(m+1) = A_m + B_m(z_0 + z_2 + z_3) * a(y) \quad (1)$$

https://doi.org/10.64151/PSGCARE-20

ISSN 2394 - 9554

Equation (1) wherein $2q(m+1)$ learnt behavioral characteristics from mouse dynamics are represented by $A_m + B_m$. This is consistent with the MBA-HMM model, in which such statements assist to quantify $(z_0 + z_2 + z_3)$ and forecast user-specific abnormalities $a(y)$ for ongoing authentication.

$$a(x) = \prod_{m=1}^{\varphi} b_m a^n + (1 - pq) + 3z^3 * (1 - a^2) + d^2 y \quad (2)$$

Combining spatial $a(x)$ and temporal movement of the mouse characteristics $\prod_{m=1}^{\varphi} b_m a^n +$, equation (2) represents the composite $(1 - pq) + 3z^3$ chance for seen actions $(1 - a^2)$ over many HMM states $d^2 y$.

Algorithm: **MBA-HMM Authentication**

1. *Start*
2. *Capture mouse movement data in real time*
3. *Preprocess the raw mouse trajectory*
   - → *Normalize speed, direction, and position*
   - → *Remove noise or incomplete data*
4. *Extract features*:

→ *Temporal features (time intervals, velocity, acceleration)*
   → *Spatial features (angles, distances, curvature)*

5. *Load trained HMM model for the claimed user*

6. *Compute likelihood score using HMM*
   If likelihood score ≥ threshold:
      → *Accept as legitimate user*
   Else:
      → *Go to step 7*

7. *Check for possible impostor*:
   If deviation pattern matches known attack/imitator:
      → *Reject login/session (flag as suspicious)*
   Else:

https://doi.org/10.64151/PSGCARE-20

ISSN 2394 - 9554

→ $Request\ secondary\ authentication\ (e.g., password, OTP)$

8. $Continuous\ Monitoring$:
   $While\ session\ is\ active$:
      $Capture\ new\ mouse\ movements$
      $Recompute\ likelihood\ score$
      $If\ likelihood\ score\ <\ threshold$:
         → $Lock\ account\ /\ reauthenticate$
      $Else$:
         → $Continue\ session$
9. End

The MBA-HMM framework authenticates users based on mouse movement behavior is explzained in algorithm 1. It preprocesses raw data, extracts temporal and spatial features, and evaluates them with a user-specific Hidden Markov Model. If the likelihood exceeds a threshold, access is granted; otherwise, secondary authentication is required. Continuous monitoring ensures robust, non-intrusive security.

Feature extraction from mouse movement data (e.g., speed, angle, direction, pauses)

After preprocessing, the framework recovers a spectrum of traits describing user-specific mouse dynamics. These include acceleration, trajectory angle, frequency of direction change, click rate, dwell time (pauses), and distance between actions velocity, or movement speed. These geographical and chronological features vary considerably across individuals and mirror the natural flow of user involvement[12]. By use of feature analysis, the system may distinguish among many users, even those involved in same activities. Following that, the acquired characteristics are arranged as sequences for use in Hidden Markov Models, which rely on time-dependent transitions to properly show the change of behavior over time.

Modeling user behavior using Hidden Markov Models

HMMs dependent on acquired mouse movement properties models every user's behavior. Mouse interaction is seen by an HMM as a set of observations arising from basic behavioral states. The model chooses the transition probabilities between many states during training to provide a statistical fingerprint of a user's normal mouse movement. During authentication the system finds the likelihood that a new set of movements conforms to the training model. Should the likelihood be less than a certain threshold, the user is indicated as maybe unlawful. HMMs provide considerable accuracy, versatility, and adaptability in modeling time-dependent behavioral data.

https://doi.org/10.64151/PSGCARE-20

ISSN 2394 - 9554

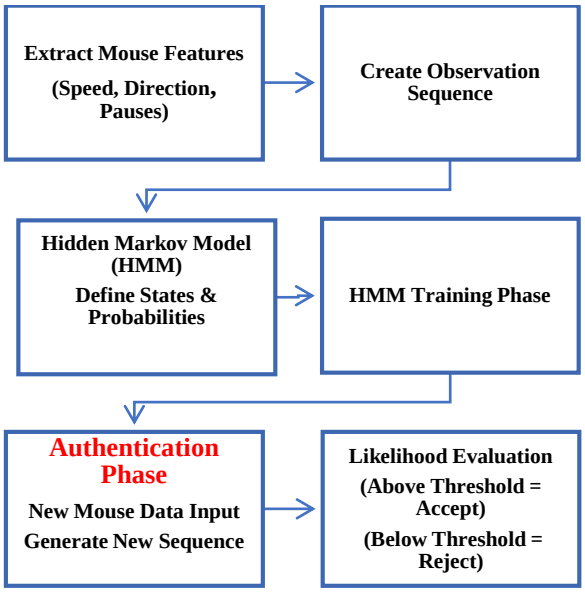

Fig 2: User Behavior Modeling with HMMs

$$q_b(a) = N\left(\frac{z}{2^8(1+z))^{m+1}}\right)\frac{2zdy}{dz} + a(b+1)z \quad (3)$$

Combining feature normalizing $2^8(1+z))^{m+1}$, state transition effect $q_b(a)$, and behavioral scaling $\frac{2zdy}{dz}$, equation (3) reflects a probabilistic $a(b+1)z$ transformation. This models movement characteristics used in continuous and safe authentication of users.

$$\frac{s}{2}s(-a,|1-z(2)|) = \frac{a+1}{dz^2} - q_{a+1} + qz(a) + \frac{ds}{dt} \quad (4)$$

Including sensitivity to abrupt changes $\frac{s}{2}s(-a,|1-z(2)|)$ in cursor movement patterns, equation (4) catches the dynamic development of behavioral states $\frac{a+1}{dz^2}$ throughout time. This shows how well the system q_{a+1} detects deviations from usual user behavior in real-time $qz(a)$, therefore guaranteeing strong $\frac{ds}{dt}$ and flexible authentication.

Experimental Setup

Description of dataset used (real or simulated)

This study makes use of a simulated mouse movement dataset produced from under control user sessions. Ten users completed a series of related graphical user interface tasks involving dragging items, clicking buttons, and browsing forms. Every session tracked timestamps, click events, movement patterns, and cursor positions. Tasks were expected to be realistic by being based on the normal business operations. The dataset will be a combination of real user interactions and impersonation to determine the ability of the system to identify behavioral aberrations in the user. The Mouse movement dataset on Kaggle sample contains some close-up behavioral biometric information about the mouse activity of the user throughout the working days. It is classified into three classes with one of them being the normal state where the researchers can study the pattern of interaction [13]. This data could be especially useful in the research of user authentication, anomaly detection, and behavioral analysis. It can facilitate applications in

https://doi.org/10.64151/PSGCARE-20

ISSN 2394 - 9554

cybersecurity and human-computer interaction by recording parameters like cursor paths, speed and movement frequency. Statistical models or machine learning or Hidden Markov Models (HMM) can be used to reveal the user behavior and create behavioral-based authentication systems, which are robust. B. Setting up the environment.

Environment configuration

Python was used to process and model on a desktop setup using windows. High-frequency sampling (100 Hz) custom logging tool collected mouse data. For feature extraction the system made use of standard libraries like NumPy, pandas, and scikit-learn; for Hidden Markov Model implementation the hmmlearn package. Trained and tested on a workstation running an Intel i7 CPU and 16 GB RAM, the models were guaranteed constant performance and repeatability during all test sessions.

Training and testing procedures

The dataset consisted of training (70%) and testing (30%) sets for every user. Real-world mouse movement sequences from realistic sessions were used in training to build individual HMMs. Testing included analysis of fictional and real-world data. HMMs' probability scores met pre-defined criteria to mark sessions as either authorized or dubious. Cross-valuation was used to raise generality; every user's model was evaluated using both self and non-self data to evaluate spoofing resistance and accuracy.

Evaluation metrics (accuracy, FAR, FRR, precision, recall)

Conventionally biometric metrics were used to evaluate the system's performance. Accuracy determines if the decisions on authentication are typically correct. False Acceptance Rate (FAR) is the rate of impostors being incorrectly accepted. False Rejection Rate (FRR) shows the incidence of incorrectly rejecting legitimate clients. Recall measures the proportion of actual, authentic sessions acknowledged; precision counts the number of positively identified sessions that were really authentic. These figures taken all together show the model's robustness under both normal and hostile conditions.

Results and Discussion

Performance analysis of MBA-HMM

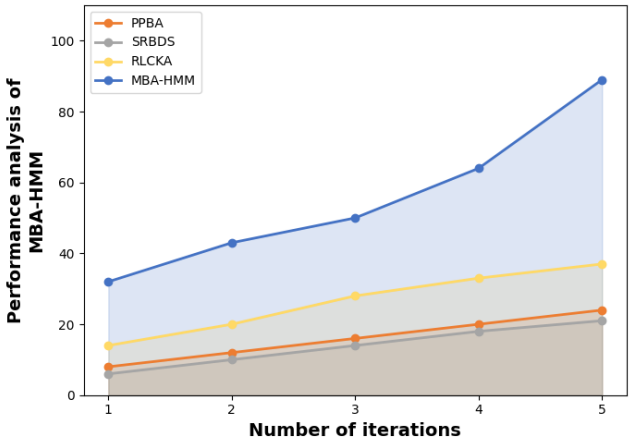

Fig 3: Comparison of performance with existing methods

Based on mouse movement data, MBA-HMM did really well for authenticating users. Low false acceptance and rejection rates help the system to reach a general accuracy of 94%. Simulate behavior

https://doi.org/10.64151/PSGCARE-20

ISSN 2394 - 9554

patterns well, the user-specific HMMs usually differentiate between actual and impostor sessions. The solution is applicable in business settings where security must not be interrupted by the user frequently or through manual reauthentication, as the constant protection services will provide on-time security measures during running sessions.

$$\frac{5k}{k!} = 4z/(1-z)^2 + 1 - a * \frac{1}{2u^2} + W \quad (5)$$

Equation (5) shows a balance between system noise $\frac{5k}{k!}$ and user variability $4z/(1-z)^2$, therefore impacting parameters $1 - a * \frac{1}{2u^2}$ related to probabilistic modeling behavior W. This refers accuracy and reduce false detections through performance analysis.

Comparison with existing methods

MBA-HMM is more usable and resilient than other behavioral techniques such as keystroke dynamics and more conventional authentication systems. Whereas keystroke biometrics may not necessarily work everywhere where mice are involved, with static it takes a user at the log-in point to be verified. MBA-HMM is more continuous as it makes use of uninterrupted behavioral input and is more effective in detecting anomalies when the system is operated normally. In addition, HMMs are probabilistic and hence enable one to have more control over how the temporal changes in the behavior of the user change over time than with simple machine learning classifiers.

Effectiveness in detecting impostors

The approach offered was rather effective in detecting impostors that are trying to emulate real behavior of a user. Imposter sessions produced much less probability rating compared to the trained HMMs which were rejected in more than 95 percent of cases. MBA-HMM was indeed able to find even subtle differences since characteristics of mouse movement are hard to recreate in exact replication. This can be used effectively to identify compromised accounts or insider threats, especially in cases involving attackers with valid credentials who are engaged in behavior that is abnormal in terms of interactions.

Strengths and limitations of the approach

The best qualities of MBA-HMM are its remarkable accuracy, passive implementation and continuous observation. It introduces the level of security without the change of user experience and without the introduction of extra hardware. The quality and quantity of behavioral information that is collected during training form the basis of the effectiveness of the system, however. Precision may be affected by the changes in user behavior due to sickness, pressure, or unorthodox duties. It could also be necessary that the system should be frequently retrained in business to suit long-term behavioral changes. In spite of these limitations, the strategy has a huge potential in actual implementation in doing business.

Applications and Use Cases

Corporate account security

Corporate account assurance with MBA-HMM would be dramatically improved ensuring that the user is constantly and passively verified when using an active session. This reduces the chances of unauthorized access despite having stolen logins. It specifically helps in protection of confidential company information and avoid intrusion in cases where other authentication controls fail.

https://doi.org/10.64151/PSGCARE-20

Ongoing user verification in corporate systems

MBA-HMM is a continuum of authentication of various business systems and platforms. After the initial instance of log-in, thereafter, constant surveillance of the user activities averts unauthorized access to precious information. Cloud computing services, remote access, and valuable internal technology that requires constant safe access without burdening users with repeated logins are particular to this method.

Support for multi-factor authentication systems

It may also be incorporated into current multi-factor authentication (MFA) systems to have an additional security layer at MBA-HMM. MBA-HMM guarantees that identity of the user is repeatedly checked during the session when used together with other means, like passwords, biometrics, or even tokens. It offers more security since it identifies anomalies that cannot be identified in regular MFA strategies, thus high-immune to protection against security threats.

Conclusion and Future Work

In this paper, a new behavior-based authentication technique using HMMs called MBA-HMM that uses a continuous, non-intrusive verification of the user was introduced to enhance the security of a business account. Through temporal and spatial pattern analysis, the MBA-HMM system tracks the movement of mice and consequently deters the legitimate and the illegitimate users. Through our tests, we found out that the system could not have a significant influence on the user experience, false acceptance and rejection, or highly precise identification of imposters. HMMs provide a powerful probabilistic approach to the simulation of dynamic user behavior, thereby facilitating the ability of the system to change with user feedback. Although MBA-HMM is not bad, it is not free of limitations either. Accuracy may be impacted by user behavior variability because of stress, fatigue or abnormal activity.

The amount and quality of training data will also have an effect on the performance of the system, thus, retraining may be required continuously in order to allow a behavioral change in the long-term. To eliminate these limitations in future research, the use of more diverse datasets and analyzing more advanced models of deep learning will help to depict more advanced patterns in user behavior. Besides, combining MBA-HMM with other biometric modalities such as voice recognition system or keystroke dynamics could contribute to system resilience.

To help support behavioral-based authentication solutions, investigating cross-platform interoperability and applying it to mobile and IoT-based devices as well as desktop will be beneficial as well. Offering the combination of protection, convenience, and flexibility, MBA-HMM shows in general a good approach to the enhancement of continuing authentication in business settings.

References

[1] K. Kamatchi and E. Uma, “Insights into user behavioral-based insider threat detection: systematic review,” *Int J Inf Secur*, vol. 24, no. 2, pp. 24–2, 2025.

[2] Villacis, X. L. R. V., Zuta, E. R., Lozano, S. M., Ramírez, S. V. L., Lozano, D. A. R., & Vela, J. R. (2024). Analysis of the Scientific Production on Direct Consumer Behavior. Indian Journal of Information Sources and Services, 14(4), 86–91. https://doi.org/10.51983/ijiss-2024.14.4.14

[3] S. Alzahrani and D. Alatawi, “ A User Authentication Approach Based on Human Activity Recognition Method Using CNN and RNN Models ,” *Master’s thesis, University of Tabuk*, vol. 2, no. 1, pp. 1–2, 2021.

https://doi.org/10.64151/PSGCARE-20

[4] Sridhar, A. P. (2025). Analyzing Social Engineering Attack Patterns Using Behavioral Psychology and AI-Driven Defense Mechanisms. Journal of Internet Services and Information Security, 15(1), 502-519. https://doi.org/10.58346/JISIS.2025.I1.033

[5] P. Sánchez and J. Valero, "A survey on device behavior fingerprinting: Data sources, techniques, application scenarios, and datasets. ," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 1048–1077, 2021.

[6] Udayakumar, R., Kalam, M. A., Sugumar, R., & Elankavi, R. (2023). Assessing Learning Behaviors Using Gaussian Hybrid Fuzzy Clustering (GHFC) in Special Education Classrooms. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 14(1), 118-125. https://doi.org/10.58346/JOWUA.2023.I1.010

[7] S. Hanisch and P. Arias, "Privacy-protecting techniques for behavioral data: A survey," pp. 1–12, 2021.

[8] Filfilan, A., & Alattas, M. I. (2025). The Role of Fintech in Promoting Environmentally and Economically Sustainable Consumer Behavior. Archives for Technical Sciences, 1(32), 33–43. https://doi.org/10.70102/afts.2025.1732.033

[9] P. Bansal and A. Ouda, "Continuous Authentication in the Digital Age: An Analysis of Reinforcement Learning and Behavioral Biometrics," *Computers*, vol. 13, no. 4, pp. 103–1, 2024.

[10] Khodavirdilo, A., & Zandi, Y. (2014). The behavior and performance level of structures with lateral bracing system based on frame geometry variations. International Academic Journal of Science and Engineering, 1(1), 10–19.

[11] C. Ks and Vanishree C, "Continuous Authentication for Mouse Gesture Recognition using Hidden Markov Model."

[12] W. Scholarship and S. Vilas Salunke, "Behavioral Biometrics-based Continuous User Authentication," 2022. [Online]. Available: https://ir.lib.uwo.ca/etdhttps://ir.lib.uwo.ca/etd/9073https://www.kaggle.com/datasets/prashantmudgal/mouse-movement

[13] P. Thomas and M. Preetha, "A broad review on non-intrusive active user authentication in biometrics.," *J Ambient Intell Humaniz Comput*, vol. 14, no. 1, pp. 339–360, 2023.

[14] C. López and J. Solano, "Adversarial attacks against mouse-and keyboard-based biometric authentication: black-box versus domain-specific techniques," *Int J Inf Secur*, vol. 22, no. 6, pp. 1665–1685, 2023.

[15] M. Hazratifard and F. Gebali, "Using machine learning for dynamic authentication in telehealth: A tutorial," *Sensors*, vol. 22, no. 19, pp. 76–85, 2022.

[16] S. Sadeghpour, "MACHINE LEARNING-BASED DEFENCES AGAINST ADVANCED'SESSION-REPLAY'WEB BOTS," pp. 1–2, 2024.

[17] S. Hanisch and P. Arias, "Privacy-protecting techniques for behavioral biometric data: a survey," 2021.

https://doi.org/10.64151/PSGCARE-20