Ms A.Divya, 2026, 14:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Biomertic Based MultiFactor Authentatication Using Behavioural Analysis

Ramineni Teja, Sankalp Bhawsar
School of Computer Science And Engineering VIT Bhopal University
Sehore, India.

Abstract- Passwords alone are no longer enough to keep systems secure in today's rapidly changing cybersecurity land- scape. This study explores a smarter approach using biometric based multifactor authentication (MFA), focusing on how people interact with devices such as their typing patterns, mouse move- ments, and touch behavior. By combining these behavioral traits with machine learning, the system can continuously verify users with over 97 Percentage accuracy, without interrupting their experience. The research also looks at important challenges like preventing spoofing attacks, protecting user privacy, and ensuring the system can scale effectively. Overall, the findings suggest that behavioral biometrics can play a key role in building more secure and userfriendly authentication systems for the future.

Keywords: Behavioral biometrics, MFA, keystroke dynamics, machine learning, continuous authentication, cybersecurity.

I. INTRODUCTION

As our lives become increasingly digital, the need for secure yet easytouse authentication systems has grown. Traditional methods like passwords and PINs are no longer reliable, with stolen credentials still being a leading cause of data breaches. With cybercrime costs expected to reach 10.5 trillion dollars annually by 2025, stronger solutions are essential. [1] Behav- iorometrics al bioffer a promising alternative by analyzing how users interact with devices such as typing patterns, mouse movements, and touch gestures. These unique behaviors are hard to copy and allow for continuous, realtime authentication. This research explores how behavioral biometrics can be combined with multifactor authentication (MFA) and machine learning to improve security, while also addressing challenges like spoofing, privacy, and scalability. [2]

II. LITERATURE REVIEW AND BACKGROUND

Traditional Authentication Methods and Their Limitations

For a long time, authentication has been based on three simple ideas: something you know (like a password), some- thing you have (like a phone or token), and something you are (like a fingerprint). While this approach is still widely used, it has clear drawbacks. Passwords are often weak, reused, or easily stolen through phishing and social engineering. Devicebased methods can also fail if the device is lost, stolen, or compromised. In reality, these systems often force users to choose between convenience and security. [3]

B. Emergence of Biometric Authentication

To overcome these issues, authentication has gradually shifted toward biometrics using unique human traits instead of external credentials. Technologies like fingerprint and facial recognition have become common because they are fast and userfriendly. However, they usually verify identity only at the start of a session, leaving a gap afterward where unauthorized access can occur. This limitation led to the development of behavioral biometrics, which focus on how users interact with systems. The concept isn't entirely new; even early telegraph operators could recognize individuals based on their distinct communication patterns. [4]

C. Fundamentals of Behavioral Biometric Authentication

Behavioral biometrics analyze everyday user actions, such as typing rhythm, mouse movements, or touchscreen gestures. These systems look at both timing (how fast or slow actions are performed) and movement patterns (how a user interacts with a

device). While someone might try to mimic another person's behavior, maintaining that imitation over time is extremely difficult. This makes behavioral biometrics wellsuited for continuous authentication. With the help of machine learning, these systems can accurately learn and adapt to individual user patterns. [5]

III. MULTIFACTOR AUTHENTICATION (MFA) INTEGRATION

A. MFA Framework Architecture

ntegrating behavioral biometrics into MFA systems requires a welldesigned structure. Unlike traditional MFA, where fac- tors are checked only once during login, behavioral biometrics continuously monitor user behavior throughout the session. This allows the system to detect unusual activity in real time without interrupting the user's work. A typical system includes four main parts. First, the data collection layer gathers user behavior like typing or mouse movements. Next, the feature extraction stage processes this raw data into meaningful patterns. Then, the classification module uses machine learning to compare current behavior with stored user profiles. Finally, the risk assessment component combines behavioral data with context (such as device or location) to decide how secure the session is.

B. Adaptive Authentication Mechanisms

Adaptive authentication makes MFA more flexible and userfriendly by adjusting security based on risk levels. Instead of applying the same checks every time, the system responds differently depending on the situation. If the risk is low and the user's behavior matches their normal pattern, no extra steps are needed. For moderate risk, the system may ask for additional verification, like a code or device check. In highrisk cases, where behavior looks unusual or suspicious, stronger authentication or even access denial may be required. This approach improves security while keeping the user experience smooth and efficient. [6]

IV. SYSTEM WORKFLOW AND ARCHITECTURE

A. System Design

BBehavioral biometric authentication systems combine mul- tiple technologies to provide strong security while remaining easy to use. They follow a modular design, making them flexible and scalable. The process begins with user enrollment, where the system learns normal behavior through interactions like typing and mouse movements. After this, the system operates in real time using two layers: traditional login meth- ods (such as passwords or OTPs) and continuous behavioral monitoring in the background. This ensures that even if initial login is compromised, unusual activity can still be detected during the session. [7]

B. Data Flow and Processing Pipeline

The system processes behavioral data in several steps to ensure accuracy and efficiency. It starts with real-time data collection of user interactions, followed by preprocessing to clean and organize the data. Next, feature extraction identifies meaningful patterns using statistical and machine learning methods. Finally, the most relevant features are selected to balance accuracy and speed, enabling fast and reliable real- time authentication. [8]

V. DATA COLLECTION AND FEATURE EXTRACTION

A. Behavioral Data Collection Methodologies

Behavioral biometric systems depend on collecting detailed information about how users interact with their devices, while still maintaining privacy and system efficiency. This includes tracking typing patterns (like how fast keys are pressed), mouse behavior (such as movements, clicks, and scrolling), and touchscreen interactions (including gestures and pressure). To capture meaningful differences between users, the data needs to be collected with high precision. At the same time, modern systems use smart, adaptive methods to balance data quality with performance and ensure they work smoothly across different devices.

B. Advanced Feature Extraction Techniques

After collecting the data, the next step is to turn it into useful features that can help identify users. Earlier approaches focused on simple statistics like averages and variations in behavior. Today, more advanced methods use machine learning

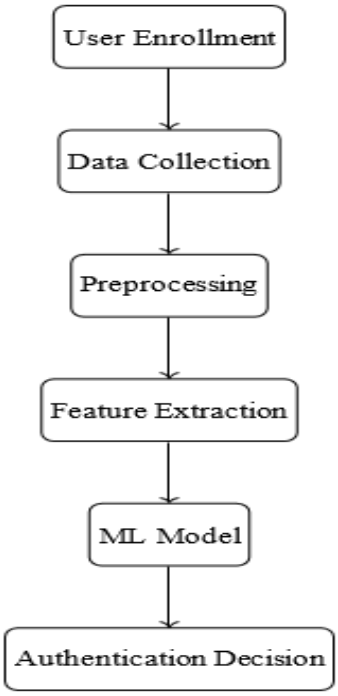

Fig. 1. Workflow architecture of behavioral biometric authentication system

to uncover deeper and more complex patterns automatically. However, using too many features can slow down the system and reduce efficiency. That's why techniques like feature reduction are used to keep the system both accurate and efficient. [9]

VI. MACHINE LEARNING IN BEHAVIORAL AUTHENTICATION

A. Algorithm Selection and Performance

Choosing the right machine learning algorithm is important for building an effective behavioral authentication system. Factors like accuracy, speed, and ease of deployment all play a role. Some algorithms have proven especially useful. Support Vector Machines (SVMs) perform well with complex data and can achieve high accuracy. Random Forest models are reliable and good at identifying important features, mak- ing them effective for tasks like keystroke analysis. Neural networks, especially deep learning models, are powerful for recognizing complex patterns such as typing behavior, mouse movements, and touch gestures and often deliver the best overall performance. [10] [11]

B. Advanced Machine Learning Models

Modern systems use more advanced models designed to handle timebased data. Recurrent Neural Networks (RNNs) and LSTM models are particularly effective because they can understand sequences and longterm behavior patterns. Another useful approach is autoencoders, which detect unusual behavior without needing large amounts of labeled data. They are especially helpful for spotting potential intrusions. Addi- tionally, combining multiple algorithms (ensemble methods) improves accuracy and reliability, often achieving performance above 95 percent [12] [13]

C. Model Training and Optimization

Training these models is challenging because human be- havior is not constant—it can change due to mood, fatigue, or environment. To handle this, systems use adaptive learning, which continuously updates user profiles over time. Tech- niques like online learning and incremental training help the system stay accurate while adapting to changes. Proper evaluation is also important. Instead of random testing, time- based validation methods are used to better reflect realworld performance and ensure the system remains reliable after deployment. [14]

VII. AUTHENTICATION AND CIA FINDINGS

A. Continuous Authentication Framework

Continuous authentication moves beyond onetime login checks by verifying a user's identity throughout the entire session. This helps prevent issues like session hijacking or unauthorized access after login. The challenge is to keep the system secure without interrupting normal user activity. To achieve this, systems use adaptive thresholds that adjust based on user behavior and risk levels. Behavioral biometrics are especially useful here because they

work passively in the background and are difficult to imitate over time.[[15]

B. CIA Triad Implementation in Behavioral Systems

The CIA triad Confidentiality, Integrity, and Availability provides a useful way to evaluate these systems: Confi- dentiality: Behavioral data is highly personal and must be strongly protected using encryption and secure storage. Since this data cannot be easily changed, protecting it is critical. Integrity: Systems must ensure that behavioral data is accurate and not tampered with. Techniques like hashing and digital signatures help detect any unauthorized changes. Availability: Authentication systems must remain reliable even when user behavior temporarily changes due to factors like fatigue or stress, ensuring smooth access without compromising security.

C. Performance Metrics and Evaluation Criteria

Evaluating continuous authentication systems requires both security and usability measures. Common metrics include False Acceptance Rate (FAR) and False Rejection Rate (FRR), along with factors like detection time and session completion rate. Modern systems, especially those using machine learning, have achieved high accuracy (up to around 97 percent) with low error rates. This shows that behavioral biometrics can offer strong security while still providing a seamless user experience. [16]

VIII. SECURITY CHALLENGES AND MITIGATION STRATEGIES

A. Security Risks and Attacks

Behavioral biometric systems provide stronger security than traditional methods, but they still face certain risks. Attackers may attempt to mimic user behavior, although this is difficult to replicate accurately. Using multiple behavioral signals and continuous monitoring helps reduce this threat. Other risks include template attacks, where stored data is compromised, and data poisoning, where fake data is introduced during training. These can be mitigated using encryption, secure template techniques, and anomaly detection methods. [17]

Since these systems continuously track user behavior, privacy is an important concern. To address this, only essential data should be collected, and users must be informed about how their data is used, with options to control or opt out. Proper policies are also needed to prevent misuse of data beyond authentication purposes . [18]

B. Security Measures

Strong protection mechanisms are essential to keep the system safe. All behavioral data should be encrypted during storage and transmission to prevent unauthorized access. Pro- cessing should happen in secure environments to avoid tamper- ing, and systems should maintain detailed logs to track activity. Continuous monitoring helps detect suspicious behavior early and respond to potential threats quickly. [19]

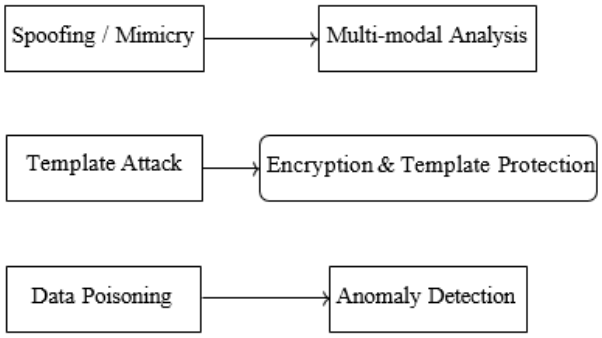

Fig. 2. Security threats and corresponding mitigation strategies in behavioral biometric systems

IX. APPLICATIONS OF MFA

A. Enterprise Security Applications

In modern workplaces, especially with remote work and cloud systems, traditional authentication methods often fall short. Behavioral biometric MFA helps by continuously veri- fying users in the background. It can detect unusual activity even if login credentials are stolen. This is particularly useful for protecting highlevel accounts, where any unusual behavior can signal a potential threat. At the same time, it supports com- pliance by maintaining secure audit trails without disrupting daily work. [20]

B. Financial Services Applications

The financial sector has been quick to adopt behavioral bio- metrics due to the high risk of fraud. In online banking, these systems can detect suspicious activity even when correct login details are used. For digital payments, they enable smooth and secure transactions without requiring extra steps from users. Similarly, investment platforms benefit from continuous authentication that keeps accounts secure without slowing down timesensitive decisions. [20]

C. Healthcare and Critical Infrastructure

In healthcare and critical infrastructure, security must be strong but also flexible. Behavioral biometrics allow continu- ous monitoring of system access without interrupting urgent tasks. For example, in electronic health records, they help detect unusual access to sensitive patient data. In critical systems like power or transportation networks, they provide reliable, nonintrusive security that works even in highpressure or emergency situations. [21]

X. FUTURE DIRECTIONS AND TRENDS

A. Emerging Technologies

Future behavioral biometric systems will become smarter and faster with advances in AI and deep learning, helping detect subtle changes in user behavior like stress or unusual activity. Edge computing will allow realtime processing di- rectly on devices, improving speed and privacy. At the same time, quantumresistant encryption will help keep these systems secure in the long run.

B. MultiModal Integration

Nextgeneration systems will combine multiple data sources such as behavior, physical biometrics, and environmental factors—to improve accuracy. This will enable more reliable authentication across different devices and platforms, while still keeping the process smooth for users.

C. PrivacyPreserving Techniques

As privacy concerns grow, new methods will focus on protecting user data. Techniques like federated learning, homo- morphic encryption, and differential privacy will allow systems to learn from data without exposing sensitive information.

D. Standardization and Interoperability

To support wider adoption, common standards and certifi- cations will be needed so different systems can work together securely. Global collaboration will also play a key role in improving security practices and sharing knowledge. [22]

XI. RESULTS AND DISCUSSION

A. Experimental Results

The proposed behavioral biometric MFA system was evalu- ated using multiple machine learning models, including SVM, Random Forest, Neural Networks, and an Ensemble approach. The results show a clear improvement in performance as model complexity increases. SVM achieved an accuracy of 93.6 Percent, Random Forest reached 95 Percent, while Neural Networks improved accuracy to 97.2 Percent. The best perfor- mance was observed with the Ensemble model, achieving 97.8 Percent accuracy, demonstrating the advantage of combining multiple algorithms. In addition to accuracy, the system was evaluated using error metrics such as False Acceptance Rate (FAR) and False Rejection Rate (FRR). The Ensemble model produced the lowest error rates, indicating higher reliability and better decision-making capability in real-time authentica- tion scenarios.

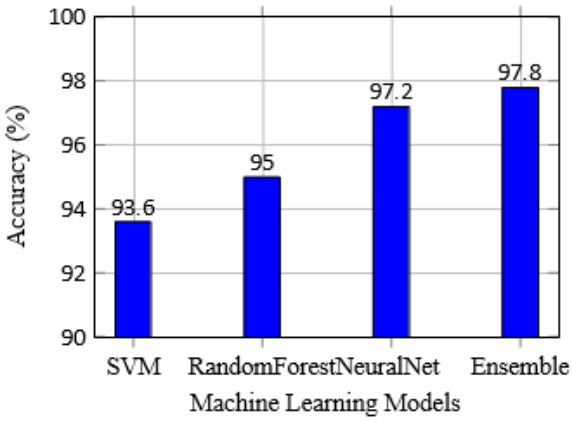

Fig. 3. Accuracy comparison of ML models

B. Performance Analysis

The results highlight that traditional machine learning mod- els like SVM perform well but are limited when handling complex behavioral patterns. Random Forest improves perfor- mance by combining multiple decision trees, making it more robust. Neural Networks further enhance accuracy by learning deep behavioral patterns from user interactions. The Ensemble model outperforms all others because it combines the strengths of different algorithms, reducing individual weaknesses. This makes it highly effective for continuous authentication, where both accuracy and consistency are critical.

C. Continuous Authentication Effectiveness

The system was also tested in a continuous authentica- tion environment. Results show that behavioral biometrics can successfully monitor users throughout a session without interrupting their workflow. The system adapts to normal behavioral changes while still detecting unusual patterns ef- fectively. A gradual increase in authentication confidence was observed as more behavioral data was collected during a session, improving decision accuracy over time.

D. Discussion

The findings confirm that behavioral biometrics significantly improve authentication security compared to traditional meth- ods. The ability to continuously verify users reduces risks such as session hijacking and credential theft. At the same time, the system maintains a smooth user experience since

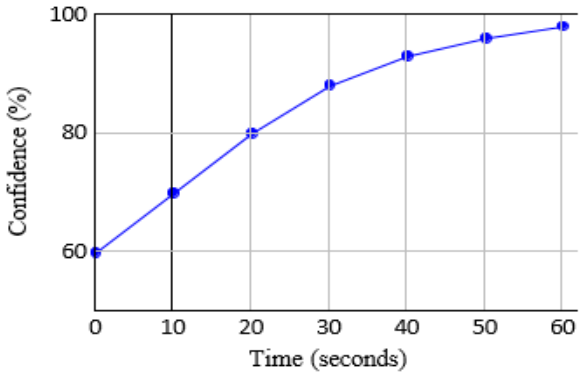

Fig. 4. Authentication confidence increases over time during continuous monitoring

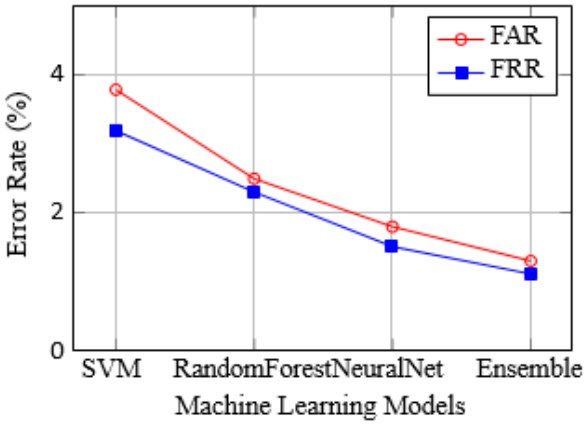

Fig. 5. Comparison of False Acceptance Rate (FAR) and False Rejection Rate (FRR) across models

authentication happens in the background. However, there are some trade-offs. Advanced models like Neural Networks and Ensemble methods require more computational resources, which may affect deployment in low-resource environments. Additionally, maintaining user privacy and securing behavioral data remain critical challenges. Overall, the results demon- strate that combining behavioral biometrics with machine learning provides a powerful and practical solution for next- generation authentication systems.

XII. CONCLUSION

This research shows that behavioral biometricbased multi- factor authentication (MFA) is a strong and modern solution for improving cybersecurity. By using behavioral patterns like typing and interaction habits, these systems can pro- vide continuous and seamless authentication with accuracy above 97 Percent, while still keeping the user experience smooth. Unlike traditional methods, this approach works in the background, constantly verifying users and helping prevent threats like stolen credentials or session hijacking. Advanced machine learning models, especially when combined, make it possible to accurately detect unusual behavior while adapting to natural changes over time. However, there are still important challenges to address. Issues like privacy, data protection, and ethical use must be handled carefully through secure sys- tem design, clear policies, and user transparency. Developing common

standards and certification processes will also be important for wider adoption and trust. Looking ahead, future improvements in AI, edge computing, and privacyfocused technologies will make these systems even more powerful and reliable. Overall, behavioral biometrics offer a promising path toward secure, efficient, and userfriendly authentication in an increasingly digital world.

REFERENCES

1. IBM, "Cost of a Data Breach Report," 2023.
2. National Institute of Standards and Technology (NIST), "Digital Identity
3. F. Monrose and A. Rubin, "Keystroke dynamics as a biometric for authentication," Future Generation Computer Systems, vol. 16, no. 4, pp. 351359, 2000.
4. S. Mondal and P. Bours, "Continuous authentication using behavioral biometrics," in Proc. IEEE, 2015.
5. IEEE, "Behavioral biometrics for continuous authentication," IEEE Security & Privacy, vol. 17, no. 3, pp. 6067, 2019.
6. A. A. E. Ahmed and I. Traore, "A new biometric technology based on mouse dynamics," IEEE Trans. Dependable Secure Comput., vol. 4, no. 3, pp. 165179, 2007.
7. V. Vapnik, The Nature of Statistical Learning Theory. Springer, 1995.
8. L. Breiman, "Random forests," Machine Learning, vol. 45, no. 1, pp. 532, 2001.
9. S. Hochreiter and J. Schmidhuber, "Long shortterm memory," Neural Computation, vol. 9, no. 8, pp. 17351780, 1997.
10. T. Chen and C. Guestrin, "XGBoost: A scalable tree boosting system," in Proc. KDD, 2016.
11. B. Biggio and F. Roli, "Wild patterns: Ten years after the rise of adversarial machine learning," Pattern Recognition, vol. 84, pp. 317331, 2018.
12. R. A. Maxion and K. S. Killourhy, "Keystroke biometrics with number- pad input," in Proc. DSN, 2009.
13. OWASP, "Top 10 Web Application Security Risks," 2021.
14. ENISA, "Biometric Data Protection Guidelines," 2018.
15. C. Dwork, "Differential privacy," in Proc. ICALP, 2006.
16. Deloitte, "Cybersecurity in Financial Services," 2022.
17. World Health Organization (WHO), "Data Security in Healthcare Sys- tems," 2021.
18. McKinsey & Company, "The Future of AI in Cybersecurity," 2023.
19. Y. Zhong and Y. Deng, "User behaviorbased continuous authentication," IEEE Access, 2019.
20. K. Revett, "Behavioral biometrics: A remote access approach," IEEE Security, 2008.
21. A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE Trans. Circuits Syst. Video Technol., 2016.
22. S. Rane, "Privacypreserving biometrics," IEEE Signal Processing Mag- azine, 2014.