WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Analysis of Behavioural Biometrics for Fraud Detection

Given Adithi Shetty, Dr Dattatreya P Mankame, Dr Basavaraj Patil, Mrs. Veena Dhavalgi

Department of Computer Science and Business Systems, Dayananda Sagar College of Engineering, Bangalore, Karnataka, India

ABSTRACT –

Fraud detection is a critical challenge faced by industries reliant on digital transactions, prompting the exploration of advanced biometric techniques. This paper presents an analysis of behavioural biometric modalities—specifically keystroke dynamics, mouse movements, in their effectiveness for detecting fraudulent activities. This study contributes empirical evidence to inform decision-making regarding the integration of behavioural biometrics into fraud detection systems, emphasizing considerations for implementation and future research directions.

Index Terms *- Behavioural biometric modalities, keystroke dynamics.*

I. INTRODUCTION

In today's digital landscape, the proliferation of online transactions has amplified the need for robust fraud detection mechanisms. Behavioural biometrics, which analyse unique patterns in user behaviour, represent a promising frontier in enhancing the security and reliability of transaction systems. This paper explores and compares the effectiveness of three primary behavioural biometric modalities – keystroke dynamics, mouse movements and voice recognition.

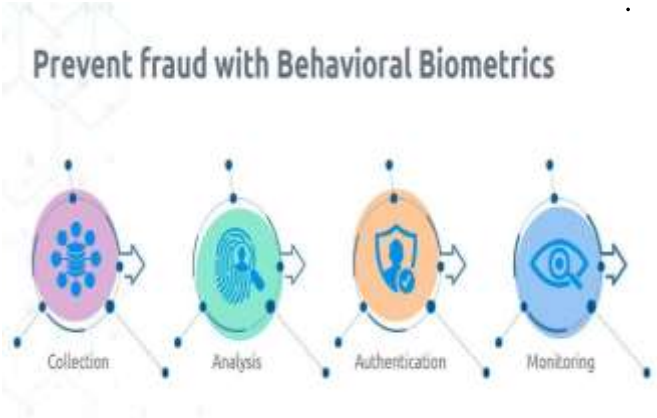
II. PRINCIPLES OF BEHAVIOURAL BIOMETRICS

Uniqueness*: Behavioural biometrics leverage the inherent uniqueness in human behaviour. Just as fingerprints and DNA are unique to individuals, behavioural patterns such as typing rhythms, mouse movements, and voice characteristics are distinctive and difficult to replicate.*

Consistency*: Behavioural biometrics exhibit consistent patterns over time for each individual, despite variations*

in environmental conditions or circumstances. This consistency allows for reliable recognition and authentication based on long-term behavioural traits.

Inherence*: Behavioural biometrics are inherent to an individual's natural interactions with devices or systems. Unlike traditional knowledge-based or possession-based authentication methods (e.g., passwords, tokens), behavioural traits are intrinsic and do not require memorization or physical possession.*



III. FEATURES USED IN EACH BIOMETRIC MODALITY

Keystroke dynamics:

Hold Time: *Duration a key is held down before release.*

Flight Time: *Duration between releasing one key and pressing the next.*

Dwell Time: *Total time a key is pressed.*

Latency Time: *Time between key releases and subsequent key presses.*

Key Pressure: *Pressure applied to keys.*

Keystroke Frequency: *Frequency of certain key combinations or sequences.*

Mouse Movement:

Path Length: *Total distance covered by the mouse cursor movements during a session.*

Average Speed: *Mean speed of mouse movements calculated as path length divided by total time.*

Direction Changes: *Number of times the mouse changes direction.*

Inter-click Time: *Time interval between consecutive clicks or movements.*

Mouse Movement Speed Variability: *Variance or standard deviation of mouse movement speeds.*

Click Duration: *Duration for which a mouse button is held down.*

IV. TECHNOLOGICAL IMPACTS OF BEHAVIOURAL BIOMETRIC MODALITIES

Behavioural biometric modalities have significant impacts across various domains, influencing both technological advancements.

Enhanced Security: *Behavioural biometrics provide an additional layer of security beyond traditional methods like passwords or PINs. They leverage unique behavioural patterns (e.g., typing rhythm, mouse movements) that are difficult to replicate, thereby enhancing authentication accuracy and reducing the risk of unauthorized access.*

Adaptive and Continuous Authentication:

Behavioural biometric systems can adapt and evolve over time based on changes in user behaviour. This capability supports continuous authentication, where users are monitored throughout their session to detect anomalies or unauthorized access attempts dynamically.

Bias and Fairness: *Biometric systems, including behavioural modalities, must address biases that may arise from demographic factors or cultural differences in behavioural patterns. Ensuring fairness in algorithmic decision-making is crucial to prevent discriminatory outcomes and promote inclusivity.*

Legal and Regulatory Implications: *The deployment of behavioural biometrics necessitates compliance with legal frameworks governing data privacy, security, and consumer rights. Organizations must navigate regulatory challenges to ensure lawful and ethical use of biometric data.*

V. COMPARISON WITH ALTERNATIVE BIOMETRIC APPROACH

Keystroke dynamics and mouse movement are distinct behavioural biometric modalities used for authentication and fraud detection. Keystroke dynamics analyse unique typing rhythms and patterns, offering non-intrusive continuous authentication but are susceptible to variability and environmental influences. Mouse movement captures detailed spatial and temporal behaviours, versatile across devices, yet sensitive to settings and complex in interpretation. Compared to fingerprint recognition, which requires physical contact but offers high accuracy, and facial recognition, which is convenient but vulnerable to environmental factors, keystroke dynamics and mouse movement provide complementary strengths in user authentication and fraud prevention, each suited to specific operational contexts and user acceptance levels. Understanding their nuances helps in leveraging these modalities effectively for enhancing security and user experience in diverse applications.

VI. CHALLENGES AND SOLUTIONS IN BEHAVIOURAL BIOMETRIC MODALITIES

Behavioural biometric modalities such as keystroke dynamics and mouse movement face several challenges that need to be addressed for effective implementation:

Environmental Factors: External conditions such as different keyboards or mouse settings can influence biometric measurements, leading to inconsistent performance. Machine learning techniques can help in recognizing and adapting to these variations.

Security and Spoofing*: Behavioural biometrics, while difficult to replicate compared to physical traits, are still susceptible to spoofing attacks through emulation or simulation of user behaviour. Continuous monitoring and anomaly detection can also help in identifying suspicious activities.*

Integration and Scalability*: Integrating behavioural biometric systems into existing infrastructures and scaling them for large user bases can be complex and costly. Cloud-based solutions can provide scalability and flexibility while reducing upfront costs.*

VII. FUTURE TRENDS IN BIOMETRIC MODALITIES

Multimodal Biometrics: *The integration of multiple behavioural biometric modalities (e.g., keystroke dynamics, mouse movement, voice patterns) with physiological or other behavioural traits (e.g., facial recognition, fingerprint scanning) is gaining traction.*

Continuous Authentication: *Moving beyond static login processes, continuous authentication monitors user behaviour throughout sessions. Advances in machine learning and AI enable systems to detect anomalies in real-time, by promptly identifying unauthorized access attempts or changes in user behaviour patterns.*

VIII. CONCLUSION

Behavioural biometric modalities such as keystroke dynamics and mouse movement represent a promising frontier in authentication and fraud detection systems. This paper has explored their strengths in providing nonintrusive, continuous authentication while highlighting challenges such as variability in user behaviour and susceptibility to environmental factors. Despite these challenges, ongoing advancements in machine learning, contextual awareness, and privacy-preserving technologies are poised to enhance the reliability and applicability of behavioural biometrics.

IX. REFERENCES

1. *Ioannis Stylios, Spyros Kokolakis, "Behavioral biometrics & continuous user authentication on mobile devices: A survey", Information Fusion, Volume 66, Pages 76-99, February 2021.*
2. *Maro Choi, Shincheol Lee, Minjae Jo, Ji Sun Shin, Sejong University, "Keystroke Dynamics-Based Authentication Using Unique Keypad", March 2021.*
3. *Akriti Verma, Valeh Moghaddam, Adnan Anwar, Deakin University, "Data-Driven Behavioural Biometrics for Continuous and Adaptive User Verification Using Smartphone and Smartwatch", 16 June 2022.*