

AI-Driver Behavioral Biometrics for Fraud Detection in  
Digital Banking systems

|                                                                  |     |
|------------------------------------------------------------------|-----|
| Abstract .....                                                   | 1   |
| Introduction .....                                               | 2   |
| Background .....                                                 | 3   |
| The evolution of digital banking and online fraud .....          | 3.1 |
| Limitation of traditional Authentication Methods in banking..... | 3.2 |
| Introduction to behavioral Biometrics .....                      | 3.3 |
| Depend on for continuous Authentication in banking systems.....  | 4.4 |
| Problem Statement .....                                          | 4   |
| Research Objectives .....                                        | 5   |
| Research scope .....                                             | 6   |
| Literature review .....                                          | 8   |
| Research Methodology .....                                       | 5   |
| Phase 1: Literature Review .....                                 | 15  |
| Phase 2: Qualitative Research .....                              | 15  |
| Phase 3: Quantitative Research .....                             | 16  |
| Phase 4: Framework Development and Validation .....              | 16  |
| Ethical Considerations.....                                      | 17  |
| Limitations .....                                                | 17  |
| Expected Outcomes .....                                          | 17  |
| Gantt chart.....                                                 | 19  |
| References .....                                                 | 20  |

## Abstract

The rapid growth of digital banking services has significantly increased the risk of online financial fraud. The traditional method of authentication such as password and codes are no longer sufficient to prevent unauthorized access that why, in this AI-Driver behavioral biometric emerged as a promising solution for continuous and invisible user authentication. In this study, reviews how machine learning and deep learning technique can analyze user as keystroke dynamic, mouse movement, and touchscreen interactions to detect fraudulent activities. This research explores the use of behavioral biometrics powered by intelligence as an advanced solution. The objective is to highlight the effectiveness, challenges, and potential of AI-driver behavioral biometrics system.

## Introduction

The rapid digital transformation of banking services has led to the widespread adoption of online and mobile banking platform financial enabling customers to perform financial transaction anytime and anywhere .while this evolution has improved accessibility and convenience, it has also significantly increased the exposure of banking system to cyber threats and financial fraud . Attackers continuously develop new technique such as phishing credential theft, malwares, and social engineering to bypass traditional authentication mechanism and gain unauthorized access to users ‘accounts.

Conventional security methods, including passwords, PIN codes, and one-time passwords (OTP), are increasingly proving insufficient to protect digital banking systems. These methods rely on static credentials that can be stolen,guessed,or intercepted .even multi-factor authentication , although more secure, may still be vulnerable to sophisticated attacks and often impacts users experience.as a result, there is a growing need for more intelligent, adaptive , and continuous authentication mechanisms capable of detecting fraud beyond the login phase. In recent years, behavioral biometrics has emerged as a promising approach to enhance digital security. Unlike physiological biometrics such as fingerprint or facial recognition, behavioral biometrics focus on how users interact with devices and systems. Feature such as keystroke dynamic mouse movement, touchscreen behavior and navigation patterns can be used to build unique behavioral profiles for each user .these pattern are difficult for attackers to replicate, making behavioral biometrics an effective tool for fraud detection.

The integration of artificial intelligent (AI) and Machine learning (ML) technique has further strengthened the potential of behavior biometrics in banking security.AI-driver models can learn normal user’s behavior, identify anomalies in real time, and continuously authenticate users during their interaction with banking application. This approach allows for invisible and non-intrusive security that enhances both protection and usability.

This literature review aims to explore how AI-driven behavioral biometrics can be used for fraud detection in digital banking system .it examines the existing technic machine learning

models, application, challenge and feature research direction in this emerging field of cybersecurity

## **The evolution of Digital Banking and online Fraud**

Over the past decade, banking services have shifted from physical branches to digital platform such as mobile and online banking .while this evolution has improved accessibility ,it has also opened new doors for cybercriminals. Among cybercrimes, phishing is a method used to obtain customer information, particularly their username and passwords

## **Limitation of traditional authentication methods in banking**

Autentification technique such as password, PIN code, and one-time passwords are widely used in banking systems however these methods are increasingly vulnerable to modern attack technique in particular, SQL injection, phishing attacks, and denial-of-services attacks are common threats. In this context , new methods are essential to combat these types of attacks.

## **Introduction to behavioral biometrics**

Behavioral biometrics has emerged as a promising security approach that focuses on how users interact with devices rather than who they are physically. Given the challenges associated with their use, it important to have systems evaluation methodologies

## **The need for continuous authentication in banking systems**

One of the major weaknesses of tradional authentication is that user verification occurs only at login time. This creates a security gap during the active session.

## **Problem statement**

Despite its promising capability it still faces several challenge including, privacy concerns, behavioral variability, mimicry attacks, data requirement real-time processing constraint, and integration difficult within existing banking infrastructure. They use of advanced authentication mechanism; banks are still unable to detect fraud when attackers use legitimate credentials to access user accounts.

## **Research objectives**

1. Understanding traditional authentication methods
2. Analyzing the weaknesses of traditional detection approaches
3. Introduction to behavior-based detection methodology
4. Analyzing its advantages and limitations

## **Research scope**

Analysis of Existing Challenges: Concentrating on identifying and understanding the key issues that currently hinder trust and transparency of AI-Driver Behavioral Biometrics for Fraud Detection in Digital Banking systems. This research focuses on behavioral data collected from user Interaction with banking application, including keystroke dynamics, touch gesture and navigation behavioral. This evaluation seeks to assess the efficacy and limitations of these solutions in addressing the identified challenges

## **Literature review**

Several researchers have explored the use of behavioral biometrics and machine learning techniques for user authentication and fraud detection. This action reviews the most relevant studies that form the Scientific foundation of this research

Work by **Isaac Adinoyi Salami** (2025) it highlight the limitation of fraud detection technique in the digital banking sector and explore the application of AI-based behavioral biometrics as a next generation solution for strengthening security

Later **Daouda Ahmet Mahamat** (2025) compared different types of keystroke dynamics and highlighted their potential for authentication systems .this study emphasized that behavioral traits are more difficult to replicate than physical

In the context of Mobil device **Kasprowski, Katarzyna Harezlak**(2018)

## **Research methodology**

This research follows a four-phase methodology combining literature analysis data collection machine learning modeling, and framework validation