



## **Title**

Prepared By

Name: ABDOURAOUF AHAMADA SAROUMAYA

ID No: M253000032

Submitted in fulfillment of the requirements for the degree Master of  
Science in Artificial Intelligence

At

Collage of Informatics

Midocean University

UAE

Supervisor Name: Dr.khaled Eskaf

Collage of Informatics, Midocean University, Comoros

Email:guilbertahamada@gmail.com

**Chapter 1: Introduction ..... 1**

1.1 Overview

1.2 Problem statement.....

1.3 Thesis Objectives.....

1.4 Thesis Contribution.....

1.5 Thesis Organization.....

**Chapter 2: background and related work.....**

2.1 Evolution of digital banking and online fraud.....

2.2 Limitation of traditional Authentication Methods in banking.....

2.3 Introduction to behavioral Biometrics.....

2.4 Depend on for continuous Authentication in banking systems.....

2.5 literature review.....

**Chapter3: Framework Development and Validation.....**

## **Chapter1:**

### **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

### **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.

### **Thesis 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

### **Thesis contribution**

Analysis of Existing Challenges: Concentrating on identifying and understanding the key issues that currently hinder trust and transparency of AI-Driven 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

## **Chapter 2**

### **Background and related work**

#### **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**

Authentication 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 is important to have systems evaluation methodologies

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

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

### **Research scope**

Analysis of Existing Challenges: Concentrating on identifying and understanding the key issues that currently hinder trust and transparency of AI-Driven 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

**Pozzolo (2017), Carcillo (2010), and Phua** demonstrate the importance of applying machine learning to bankcard fraud detection. Pozzolo show a realistic model of the problem of detection, taking into account the significant data imbalance, and introduces learning method adapted to this context. They present a comprehensive review of machine learning algorithms used for fraud detection, highlighting the performance of supervised, unsupervised, and others methods. Carcillo expands on this analysis by offering a synthesis of exist techniques for bank card fraud detection, while Phua emphasizes the importance of behavioral pattern mining in fraud identification.

However, these approaches primarily focus on analyze financial transactions without consider the behavioral identity of the user making those transactions. A second area of research focuse on the use of behavioral biometric for authentication.

Mario frank and ralf biedert (2012) demonstrated that keystroke dynamics can identify a user based on their typing rhythm. Yu Zhong and yunbin deng (2012) show that mouse movements also constitute a reliable behavioral signature. With the evolution toward touch interfaces, Frank introduce the use of touchscreen interactions as a means of continuous authentication.

**Loannis stylios and Andrea's skalkos (2022)** offer a comprehensive classification of the different behavioral biometric techniques and highlight their

strengths and weaknesses, particularly their sensitivity to variations in user behavior. This research proves that human behavior can serve as a biometric identifier, but it remains largely limited to the field of authentication and is not directly applied to bank fraud detection.

**Simon Eberz and kasper B Rasmussen** (2017) propose continuous authentication approaches using behavioral biometrics and anomaly detection techniques. This work show the possibility of closely and continuously monitoring user behavior during sessions to detect any anomaly. The use of IA models allows for the generation of real-time scores. However, these approaches often remain experimental, complex to deploy on a large scale, and very rarely integrated into real banking systems for fraud detection.

Model of detection fraud proble taking into account the significant data imbalance and introduce learning strategy adapted to this pozzolo research, published in the Journal of Industrial Information Integration

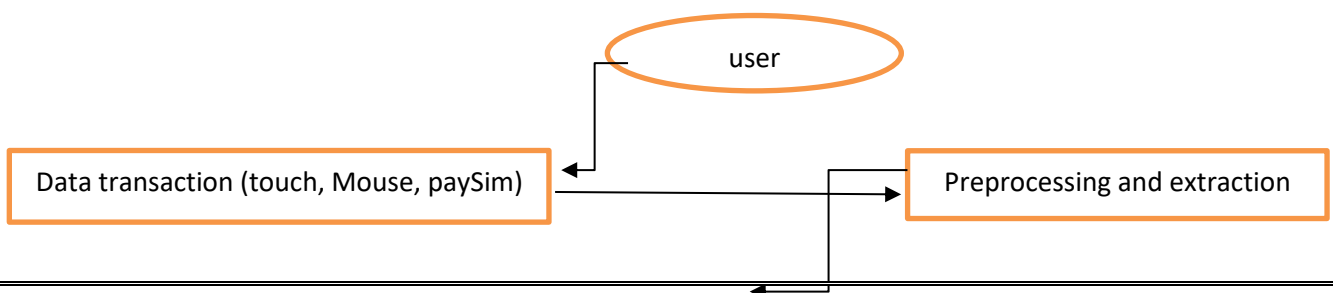
**Abdallah et al.** Explain a comprehensive review of machine learning (ML) techniques to use to bank fraud, categorized into supervised, unsupervised, and hybrid approaches. They emphasize that traditional methods (**SVM, Random Forest, and Logistic Regression**) are showing their limitations in the face of evolving fraud patterns and recommend the integration of behavioral and adaptive techniques. Carcillo et al. reinforce this idea by demonstrating that most existing systems rely solely on transactional characteristics, neglecting user behavior. They identify a clear lack of integration between bank fraud and behavioral biometrics. Phua et al. introduce the concept of Behavioral Pattern Mining, demonstrating that analyzing user habits (sequence of actions, rhythm, interactions) allows for more precise detection than purely financial analysis.

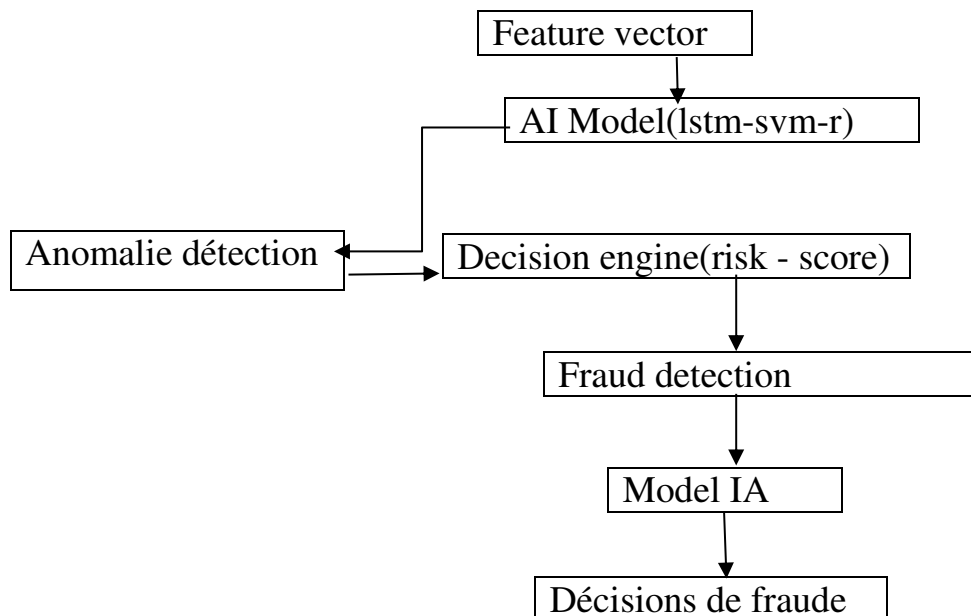
| N° | problem                     | Method used                              | limitation                                                     |
|----|-----------------------------|------------------------------------------|----------------------------------------------------------------|
| 1  | Fraud detection in banking  | Behavioral biometrics + machine learning | It not specifically adapted to real-time                       |
| 2  | Credit card fraud detection | Deep learning                            | It heavy dependent on history data and does not take real-time |

|   |                                                             |                                                                                                                            |                                                                                                   |
|---|-------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| 3 | Credit card detection                                       | Supervised and unsupervised learning                                                                                       | Based solely on transaction and ignores user behavior                                             |
| 4 | Fraud detection based on data mining                        | Review of data mining technics(classification, clustering)                                                                 | Outdated methods, focused on transactional data rather than user behavior                         |
| 5 | User authentication based on keyboard behavioral            | Behavioral biometrics and machine learning                                                                                 | Used for local authentication not integration with real-time                                      |
| 6 | Continuous authentication with touch integration on screen  | Behavioral biometrics statistical modal/machine learning                                                                   | Sensitive to usage variations and requires a large amount of data to be reliable not specifically |
| 7 | Review of behavioral biometrics technic based on keystrokes | Survey analyze of several keystrokes dynamics model + machine learning                                                     | Synthesis of existing method without propose an integration solution                              |
| 8 | Evolution of continuous authentication system               | Based on behavioral biometrics Analyze of several continuous authentication model(machine learning +behavioral biometrics) | Difficulty in achieving a balance between security and usability                                  |
|   |                                                             |                                                                                                                            |                                                                                                   |
|   |                                                             |                                                                                                                            |                                                                                                   |

## Chapter 3

### 3.1 architecture général du Framework





## 1. Detailed Framework Architecture:

This architecture proposes fraud detection in banking systems based on an intelligent processing chain based on the extraction of behavioral characteristics up to the decision based on a risk score.

This system is based on nine blocks:

### 1.1 User:

The user interacts with the banking system, and each interaction affects two types of data:

- ✓ Behavioral data
- ✓ Transactional data

### 1.2 Data transactions:

This module groups all the data generated during the session:

- ✓ History
- ✓ Actions performed
- ✓ Sequence of reactions

### 1.3 Preprocessing and feature extraction:

In this stage, the data is cleaned, normalized, and transformed:

- ✓ Noise removal
- ✓ Normalization
- ✓ Extraction of behavioral and transactional indicators

### 1.4 Feature Vector:

The extracted characteristics are grouped into a feature vector that represents the overall profile of the user's session.

### 1.5 Anomaly detection:

Model detection detects any deviation from the user's usual behavior.

### **1.6 Decision engine (risk score):**

- ✓ AI model results
- ✓ Observed anomaly levels

### **1.7 Fraud detection:**

- ✓ Normal
- ✓ Suspicious fraudulent

### **AI model (LSTM-SVM-Random Forest):**

- ✓ **LSTM:** analyzes temporal actions
- ✓ **SVM:** classifies behavior Normal and abnormal
- ✓ **Random Forest:** improved decision robustness

### **1.8 Real-time automatic decision:**

- ✓ Authorizes
- ✓ Requests verification