

PROFESSIONAL TRAINING REPORT - II

entitled

BEHAVIOURAL BIOMETRIC AUTHENTICATION SYSTEM

Submitted in partial fulfillment of the requirements for the award of
Bachelor of Engineering degree in Computer Science and Engineering with
specialization in Blockchain Technology

by

ROSHNI KOLIPAKA [Reg. No. 41613026]



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SCHOOL OF COMPUTING

SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

CATEGORY -1 UNIVERSITY BY UGC

**Accredited with Grade "A++" by NAAC | 12B Status by UGC | Approved by AICTE
JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600 119**

MAY 2024



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

CATEGORY-I UNIVERSITY BY UGC

Accredited "A++" Grade by NAAC | 12B Status by UGC | Approved by AICTE

www.sathyabama.ac.in

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Professional Training Report is the bonafide work of **Ms. Roshni Kolipaka (41613026)** who carried out the project entitled "**Behavioural Biometric Authentication System**" under my supervision from January 2024 to May 2024.

Internal Guide

Ms Lekshmi S Raveendran, M.Tech.,

Head of the Department

Dr. S. VIGNESHWARI, M.E., Ph.D.,

Submitted for Viva voce Examination held on 07/05/2024

Internal Examiner

External Examiner

DECLARATION

I, **Roshni Kolipaka (41613026)**, hereby declare that the Professional Training Report-II entitled "**Behavioural Biometric Authentication System**" done by me under the guidance of **Ms Lekshmi S Raveendran, M.Tech.**, is submitted in partial fulfilment of the requirements for the award of Bachelor of Engineering degree in Computer Science and Engineering with specialization in Blockchain Technology.

DATE: 07/05/2024

PLACE: Chennai



SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management of SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T.Sasikala M.E., Ph.D., Dean**, School of Computing, **Dr. S.Vigneshwari M.E., Ph.D., Head of the Department of Computer Science and Engineering** for providing me necessary support during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Internal Guide **Ms Lekshmi S Raveendran, M.Tech.**, for his/her valuable guidance, suggestions and constant encouragement which paved way for the successful completion of my phase-2 Professional Training.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Computer Science and Engineering** who were helpful in many ways for the completion of the project.

COURSE CERTIFICATE

MORNING SESSION (FN)	National Programme on Technology Enhanced Learning	 <b style="color: red; font-size: 1.2em;">NPTEL
Hall Ticket For	2024 Apr: CS15 Blockchain and its Applications - Online	

Candidate Name	Roshni Kolipaka					
Roll No	NOC24CS15S953400455	Seating Number	53400455			
Date of Birth	28-09-2003					
PwD Status	No	Compensatory Time Required	N.A	Scribe Required		N.A
Exam Date	Saturday, 27 April, 2024					
Reporting Time	08:00 am	Gate Closure	09:30 am			
Exam Timing	09:00 am	Shift	FN			
Test Centre Name	ION Digital Zone IDZ Kovilambakkam					
Test Centre Address	Fortune Towers, 1st and 2nd Floor, SH 109, 200 Feet Thoraipakkam Pallavaram Radial Road, Near Eachangadu signal, Kovilambakkam, Chennai, Tamil Nadu, India - 600117					
 NPTEL Coordinator						

ABSTRACT

Behavioural Biometric Authentication System introduces a novel approach to bolstering user authentication protocols in the cybersecurity realm. Traditional authentication methods often fall short in accurately verifying user identities, leaving systems vulnerable to unauthorized access. To address this challenge, the system proposes an innovative methodology that integrates continuous reinforcement learning with the analysis of keystroke dynamics and mouse movements. The strategy aims to rectify the limitations inherent in conventional authentication paradigms, particularly the susceptibility of static authentication factors like passwords or PINs to various attacks including brute force, phishing, and social engineering tactics. The approach hinges on the application of continuous reinforcement learning, a dynamic process wherein an agent learns to interact with its environment by performing actions and receiving feedback in the form of rewards or penalties. Specifically, the model scrutinizes the intricate patterns embedded within users' keystroke dynamics and mouse behaviours, capturing unique biometric signatures that serve as reliable indicators of identity. The continuous reinforcement learning model autonomously adapts to evolving user behaviours, discerning legitimate interactions from potential security threats with remarkable precision. The findings underscore the transformative potential of continuous reinforcement learning in fortifying authentication systems against unauthorized access attempts. By harnessing insights derived from users' behavioural biometrics and employing adaptive learning mechanisms, the system furnishes a formidable defense against malicious intrusions while upholding user convenience and usability. This research contributes to the advancement of behavioural biometric authentication methodologies, safeguarding digital assets and preserving user privacy in an increasingly interconnected landscape.

TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGE NO.
	ABSTRACT	vi
	LIST OF FIGURES	viii
1	INTRODUCTION	1
	1.1 Overview	
2	LITERATURE SURVEY	4
	2.1 survey	
3	REQUIREMENTS ANALYSIS	
	3.1 Objective	7
	3.2.1 Hardware Requirements	
	3.2.2 Software Requirements	8
4	DESIGN DESCRIPTION OF PROPOSED PRODUCT	10
	4.1.1 Ideation Map/Architecture Diagram	11
	4.1.2 Various stages	12
	4.1.3 Internal or Component design structure	13
	4.1.4 working principles	14
	4.2 4.2.1 Novelty of the Project	15
5	RESULTS AND DISCUSSION	17
6	SUMMARY AND CONCLUSIONS	20
	REFERENCES	21
	APPENDIX	
	A. Research Paper	23
	B. Source Code	27

LIST OF FIGURES

Figure No.	Figure Name	Page No.
4.1	Proposed RL Framework	11
4.2	Data Process Flow for RL Model	13
5.1	Heat Map	17
5.2	Training performance	18
5.3	Testing performance	18
5.4	ROC Curve (Train)	19
5.5	ROC Curve(Test)	19
1	Training dataset	34
2	Train the model	34
3	Test the model	34
4	Evaluation metrics result	34

CHAPTER 1

INTRODUCTION

1.1 OVERVIEW

In the contemporary digital landscape, safeguarding sensitive information and systems against unauthorized access has emerged as a paramount concern. Traditional methods of authentication, such as passwords and PINs, have increasingly proven inadequate in the face of sophisticated hacking, phishing, and social engineering attacks. Moreover, the cognitive burden of managing complex passwords often leads to user frustration and the adoption of weak or reused credentials, further exacerbating security risks. In response to these pressing challenges, researchers and practitioners have increasingly turned their attention towards Behavioural biometrics as a promising solution for identity verification.

Behavioural biometrics represents a paradigm shift in authentication methods by leveraging the unique patterns inherent in human behavior. Unlike traditional static credentials, such as passwords or PINs, which are prone to theft, Behavioural biometrics utilize dynamic behavioural characteristics that are inherently difficult to replicate or spoof. Among the various behavioural modalities, keystroke dynamics and mouse movements have garnered significant attention due to their unique characteristics, non-intrusiveness, and seamless integration into existing systems.

Keystroke dynamics involve the analysis of a user's typing rhythm, speed, and timing, which are influenced by factors such as muscle memory, cognitive processes, and motor skills. Similarly, mouse movements capture the nuanced nuances in cursor trajectories, including speed, acceleration, and direction changes, reflecting an individual's neuromuscular coordination and cognitive processing. By analyzing these behavioural patterns, Behavioural biometric authentication systems can accurately identify and verify users based on their unique behavioural signatures.

The advantages of Behavioural biometrics extend beyond security to encompass enhanced user convenience and usability. Users are relieved from the burden of remembering complex passwords, and authentication occurs seamlessly as part of their natural interaction with digital systems. Additionally, the non-intrusive nature of Behavioural biometrics eliminates the need for additional hardware or complex authentication procedures, enhancing the overall user experience.

This paper presents a comprehensive exploration of a Behavioural biometric authentication system that leverages keystroke dynamics and mouse movements as primary authentication modalities. We delve into the design, implementation, and evaluation of the system, highlighting its effectiveness in enhancing security while maintaining usability. Through extensive experimentation and user studies, we demonstrate the system's ability to accurately authenticate users based on their unique

behavioural patterns, paving the way for a more secure and user-friendly approach to identity verification in digital environments.

The design and implementation of our Behavioural biometric authentication system are rooted in the principles of usability, security, and adaptability. We begin by defining the scope and requirements of the system, outlining the target user base, the behavioural biometrics to be employed, and the desired security levels. Data collection from various sources, such as keystroke dynamics and mouse movements, is then conducted and analyzed to extract meaningful features.

Machine learning models are developed and trained using this data to recognize and authenticate users based on their behavioural patterns. Continuous reinforcement learning plays a pivotal role in the system, enabling dynamic adaptation of the authentication process to ensure resilience against emerging threats and changes in user behaviour. Throughout development, we emphasize integrating robust security measures and ensuring compliance with privacy regulations.

Extensive experimentation and user studies are conducted to evaluate the effectiveness of our Behavioural biometric authentication system. Performance metrics, including False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER), serve as key indicators of the system's accuracy and reliability. By minimizing both false acceptance of impostors and false rejection of legitimate users, we strive to strike a balance between security and usability.

Upon successful validation, our Behavioural biometric authentication system is deployed in real-world environments to assess its performance and effectiveness in practical scenarios. Continuous feedback collection and iterative improvements ensure that the system remains responsive to evolving user needs and security threats. Ongoing monitoring and maintenance are essential to sustain system integrity and address emerging challenges over time.

While Behavioural biometric authentication systems offer significant advantages, they are not without challenges. One such challenge is the need for robustness against adversarial attacks, where malicious actors attempt to deceive the system by mimicking legitimate user behaviour. Addressing these challenges requires ongoing research and innovation in the areas of security, machine learning, and human-computer interaction.

Behavioural biometric authentication systems, leveraging keystroke dynamics and mouse movements, offer a highly accurate and reliable method for user authentication. Their robustness, adaptability, and user-friendliness make them well-suited for addressing the security challenges inherent in today's digital landscape. By combining cutting-edge technology with human behaviour analysis, these systems pave the way for a more secure and user-friendly approach to identity verification in digital environments.

The implementation of a Behavioural biometric authentication system entails several key steps, each crucial for ensuring its effectiveness and reliability. The first step in implementing a Behavioural biometric authentication system is defining the scope and requirements of the system. This involves identifying the target user base, the behavioural biometrics to be employed, and the desired security levels. Understanding the specific needs and constraints of the system is essential for guiding subsequent design and development efforts.

Once the scope and requirements are defined, the next step is collecting and analyzing data from various sources, such as keystroke dynamics and mouse movements. This data serves as the foundation for training machine learning models to recognize and authenticate users based on their behavioural patterns. Data analysis techniques, such as feature extraction and dimensionality reduction, are employed to extract meaningful information from raw behavioural data.

With the data collected and analyzed, machine learning models are developed and trained to recognize and authenticate users based on their behavioural patterns. Various machine learning algorithms, such as support vector machines, neural networks, and decision trees, may be employed for this purpose. The choice of algorithm depends on factors such as the complexity of the data and the desired performance metrics.

A key aspect of Behavioural biometric authentication systems is their ability to adapt to evolving user behaviour and emerging threats. Continuous reinforcement learning techniques enable the system to dynamically adjust its authentication process based on feedback from user interactions. This adaptability ensures resilience against adversarial attacks and changes in user behaviour over time.

Integrating robust security measures and ensuring compliance with privacy regulations are essential considerations in the implementation of Behavioural biometric authentication systems. Encryption techniques, access control mechanisms, and secure communication protocols may be employed to protect sensitive user data and prevent unauthorized access. Additionally, measures must be taken to ensure compliance with privacy regulations, such as GDPR and HIPAA, to safeguard user privacy rights.

Once the system is developed, it undergoes extensive evaluation and validation to assess its effectiveness and reliability. Performance metrics, such as False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER), are used to measure the system's accuracy and reliability. User studies and real-world testing are conducted to evaluate the system's performance in practical scenarios.

Upon successful validation, the Behavioural biometric authentication system is deployed in real-world environments to assess its performance and effectiveness in production settings. Continuous monitoring and maintenance are essential to ensure that the system remains responsive to evolving user needs and security threats.

CHAPTER 2

LITERATURE REVIEW

2.1 SURVEY

Behavioural biometric authentication systems have emerged as a promising solution for continuous user authentication, aiming to mitigate the challenges associated with traditional methods. While most studies have focused on single behavioural modalities, recent research has explored the fusion of biometrics to enhance system performance.

[1] *Continuous authentication with feature-level fusion of touch gestures and keystroke dynamics to solve security and usability issues,2023.* A study proposed a fusion approach combining touch gestures and keystroke dynamics, demonstrating improved results in authentication accuracy. They developed the BioGames App to collect biometric data from mobile device users, utilizing feature-level fusion techniques to enhance system performance. Their findings revealed that the fusion of touch gestures and keystroke dynamics significantly improved system accuracy, effectively addressing security and usability concerns.

[2] *B2auth: A contextual fine-grained Behavioural biometric authentication framework for real-world deployment,2024.* B2auth framework was designed specifically for smartphone users, leveraging raw data from touchscreens to extract behavioural traits for authentication. Unlike previous studies conducted in controlled environments, their research focused on real-world deployment scenarios, achieving promising results in differentiating legitimate users from attackers across various app contexts.

[3] *Evaluation of Deep Learning Models for Continuous Authentication Using Behavioural Biometrics,2023.* The use of behavioural biometrics was explored for continuous authentication in mobile banking applications. Their study employed deep learning algorithms, including Multilayer Perceptron (MLP), LSTM, bi-directional LSTM, and convolutional LSTM, achieving high accuracy rates and low error rates. This underscores the potential of behavioural biometrics in enhancing the security of mobile applications.

[4] *A behavioural biometric dataset for user identification and authentication,2022.* They emphasized the utility of machine learning techniques in analysing behavioural biometric data to distinguish between legitimate and illegitimate card owners, thereby preventing identity theft. Additionally, they provided a dataset of keystroke dynamics, facilitating further research in cybersecurity applications.

[5] *Step & turn—A novel bimodal Behavioural biometric-based user verification scheme for physical access control,2022.* Step & Turn proposes a novel bimodal behavioural biometric-based verification scheme for physical access control,

addressing the evolving demands of smart physical spaces. By leveraging natural human behaviours such as single footstep and hand movement, Step & Turn achieves a True Acceptance Rate of 97.25% at a False Acceptance Rate of 0.01%, demonstrating its effectiveness in balancing usability and security requirements.

[6] *Behavioural biometrics & continuous user authentication on mobile devices: A survey,2021.* The survey provides a comprehensive overview of Behavioural Biometrics and Continuous Authentication technologies for mobile devices. It classifies behavioural biometrics technologies, analyses data collection methodologies, and reviews machine learning models' performance in continuous authentication. Additionally, it discusses vulnerabilities of machine learning models to adversarial attacks and proposes relevant countermeasures, offering valuable insights into current challenges and future trends.

[7] *CyberSignature: A user authentication tool based on behavioural biometrics,2022.* CyberSignature1 utilizes behavioural biometrics to create unique digital identities for online card transactions, enhancing security by distinguishing legitimate users from fraudsters. Implemented in Python with a machine learning algorithm, CyberSignature1 transforms user input data into unique digital identities, offering a promising solution to combat identity theft in online transactions.

[8] *A Lightweight Seamless Unimodal Biometric Authentication System,,2024.* AUBAS presents a lightweight and seamless authentication system based on discrete-time Markov chains, designed to improve user experience in Two-Factor Authentication (2FA) based on Unimodal Biometrics. By incorporating likelihood and weighting strategies, AUBAS demonstrates its efficacy in enhancing the authentication process and can be applied in various environments relying on unimodal biometric authentication.

[9] *Deep learning-based photoplethysmography biometric authentication for continuous user verification,2024.* The study proposes a novel biometric authentication approach using photoplethysmography (PPG) signals and deep learning techniques. Leveraging the unique characteristics of PPG signals, the research develops a robust and continuous user verification system, achieving high accuracy rates while addressing security concerns. By employing a Convolutional Neural Network (CNN) architecture, the system demonstrates its effectiveness in authenticating individuals based on their unique PPG patterns.

[10] *Empowering robust biometric authentication: The fusion of deep learning and security image analysis,2024.* The research presents a smart computational method for automatically authenticating fingerprints for identity verification and personal identification using deep learning techniques. By integrating Monte Carlo Dropout (MC Dropout) with convolutional neural networks (CNNs), the system achieves improved security and dependability in biometric identification. Moreover, the study proposes innovative activation functions to enhance the convergence of deep neural networks, contributing to advancements in biometric authentication.

[11] *Multi-biometric fusion for enhanced human authentication in information security,2024.* The study introduces a novel method for feature-level fusion in human biometric authentication, employing optimal feature selection using Binary chimp optimized adaptive kernel support vector machine (BCO-AKSVM). By selecting essential features and employing feature-level fusion, the proposed method achieves high performance in information security, demonstrating improved f1-score, recall, accuracy, precision, and computational efficiency compared to existing methods.

[12] *Multimodal biometric authentication method by federated learning, 2024.* This work presents a security management approach for authentication in the Internet of Health Things, utilizing two combined convolutional neural networks (CNN) for biometric identification. Leveraging Federated Learning (FL) and multimodal authentication with Photoplethysmography and Electrocardiogram signals, the approach achieves high accuracy and a low false acceptance rate, ensuring protection against unauthorized access attempts.

[13] *Biometric-based two-factor authentication scheme under database leakage,2024.* Addressing the vulnerability of existing Two-Factor Authentication (2FA) schemes to database leakage, this paper proposes a biometric-based 2FA scheme with biometric feature and secret key authentication factors. The scheme ensures authenticity and zero-knowledge even when the server's database is compromised, utilizing robust property-preserving hashing and fully homomorphic encryption techniques.

[14] *The design and evaluation of adaptive biometric authentication systems: Current status, challenges and future direction,2023.* Adaptive biometric authentication systems dynamically adjust their processes to changing environmental conditions and sample ageing to maintain recognition performance. This paper provides a systematic review of existing literature on adaptive biometric authentication, highlighting the need for further investigation into mobile and wearable devices and continuous authentication methodologies.

[15] *BAED: A secured biometric authentication system using ECG signal based on deep learning techniques,2022.* Proposing a novel biometric authentication scheme based on ECG detection, BAED utilizes deep learning algorithms, including convolutional neural networks (CNN) and long-term memory (LSTM) networks. Evaluated with both on-and off-person databases, BAED outperforms existing approaches, demonstrating superior performance in terms of identification parameters such as FMR, FNMR, FAR, and FRR.

CHAPTER 3

REQUIREMENTS ANALYSIS

3.1 OBJECTIVE OF THE PROJECT

The objective of this project is to design, develop, and implement a highly secure Behavioural biometric authentication system. By harnessing the distinct Behavioural patterns of users, including keystroke dynamics, mouse movements, the system aims to provide a seamless and efficient means of verifying user identities. Through continuous authentication throughout a session, the system seeks to bolster security measures, effectively mitigating risks associated with traditional authentication methods. Additionally, the project aims to optimize user convenience by eliminating the need for passwords or physical tokens, thereby streamlining the authentication process and enhancing overall user experience.

1. **Security Enhancement:** The primary goal is to enhance security measures for user authentication. By leveraging Behavioural biometrics, which are inherently difficult to mimic or replicate, the system aims to significantly reduce the risk of unauthorized access. This includes protecting sensitive data, systems, and resources from potential threats such as identity theft, fraud, and cyber attacks.
2. **Behavioural Pattern Analysis:** The project aims to conduct in-depth analysis and research into various Behavioural patterns exhibited by users. This involves studying characteristics such as keystroke dynamics, mouse movements, touchscreen interactions, and gait analysis. By understanding these unique traits, the system can accurately distinguish between genuine users and impostors.
3. **Continuous Authentication:** One of the key objectives is to implement continuous authentication throughout a user session. Unlike traditional authentication methods that only verify identity during login, continuous authentication monitors user behavior continuously. This proactive approach enables the system to detect anomalies or suspicious activities in real-time, thereby preventing unauthorized access even after initial login.
4. **User Experience Optimization:** While prioritizing security, the project also focuses on optimizing user experience. This involves designing intuitive interfaces and seamless authentication processes to minimize friction for end-users. By eliminating the need for passwords or physical tokens, the system aims to simplify the authentication process and enhance user satisfaction.
5. **Scalability and Reliability:** Another objective is to develop a scalable and reliable authentication system capable of accommodating varying user populations and usage scenarios. This includes ensuring high availability, performance, and resilience to handle fluctuations in user demand and system loads effectively.

6. **Compliance and Privacy:** The project emphasizes compliance with relevant regulations and standards governing user data protection and privacy, such as GDPR, CCPA, and HIPAA. This involves implementing robust security measures, encryption protocols, and access controls to safeguard user information and maintain confidentiality.

7. **Testing and Evaluation:** Throughout the project lifecycle, rigorous testing and evaluation procedures are conducted to assess the effectiveness, accuracy, and reliability of the authentication system. This includes simulated testing environments, user trials, and performance benchmarking against established metrics and criteria.

3.2 REQUIREMENTS

3.2.1 HARDWARE REQUIREMENTS

Hardware for Behavioural biometric authentication systems typically involves a variety of sensors and processing units. These sensors capture user behavior, such as typing rhythms, mouse movements, and even facial or gait recognition

- **Sensors:** Keyboards, mice, touchscreens, microphones, and cameras for capturing Behavioural data.
- **Processing Unit:** CPU or GPU for running authentication algorithms and analysis.
- **Storage:** Space for storing user profiles and authentication logs.
- **Networking Components:** Interfaces for network connectivity and secure data transmissions.
- **Embedded Systems:** For mobile devices or IoT devices, specialized hardware optimized for size and power consumption.
- **Physical Security Measures:** Enclosures, locks, and surveillance for protecting hardware.
- **Scalability and Redundancy:** Additional components for handling increased user loads and ensuring uninterrupted operation.
- **Compliance and Certification:** Hardware meeting regulatory standards for security and privacy.

3.2.2 SOFTWARE REQUIREMENTS

Software components work together to implement, operate, and maintain a Behavioural biometric authentication system effectively.

1. **Data Collection and Processing Software:** Software to collect and process Behavioural data from various sensors, such as keyboards, mice, microphones, and cameras.

2. **Machine Learning and Analysis Tools:** Tools for implementing machine learning algorithms to analyze Behavioural patterns and create user profiles.
3. **Database Management System:** A database management system (DBMS) to store and manage user profiles, authentication logs, and other relevant data.
4. **Networking Software:** Software for network communication, enabling data transmission between the authentication system and other components, including client devices and servers.
5. **Security Software:** Security software for encrypting data, ensuring secure communication, and protecting against unauthorized access or tampering.
6. **User Interface (UI) Design Tools:** Tools for designing intuitive user interfaces to facilitate user interaction with the authentication system.
7. **Testing and Debugging Tools:** Tools for testing, debugging, and validating the functionality, accuracy, and performance of the authentication system.
8. **Compliance and Reporting Software:** Software for ensuring compliance with relevant regulations and standards, as well as generating reports and audit trails for accountability and regulatory purposes.
9. **Integration and Compatibility Software:** Software for integrating the authentication system with existing IT infrastructure, applications, and platforms, ensuring compatibility and interoperability.
10. **Maintenance and Monitoring Software** Software for monitoring system health, performance, and security, as well as managing software updates, patches, and maintenance tasks.

CHAPTER 4

DESIGN DESCRIPTION OF PROPOSED PROJECT

4.1 PROPOSED METHODOLOGY

Traditional static authentication systems typically rely on fixed credentials such as passwords, PINs, or biometric markers like fingerprints or iris scans. While these methods provide a level of security, they lack the ability to adapt to changing user behavior or account for potential security breaches.

The integration of keystroke dynamics into authentication systems introduces a dynamic and behavior-based approach to user verification. Keystroke dynamics capture unique typing patterns and behaviors, such as typing speed, rhythm, and key press duration, which are inherent to individuals and can serve as reliable identifiers.

By leveraging reinforcement learning (RL) techniques, these keystroke dynamics can be used to train models for continuous authentication. Unlike static systems, RL-based authentication continuously learns and adapts to evolving user behavior over time. The RL agent analyzes the user's keystroke patterns and makes authentication decisions based on its learning from historical data and ongoing interactions.

Reinforcement learning (RL) is a subset of machine learning that focuses on training models to make decisions in uncertain or ambiguous environments. In the realm of behavioral biometrics, RL can be applied to train models to make decisions regarding a user's identity based on various behavioral patterns such as typing dynamics and mouse movements. The core concept of RL is to train an agent to make decisions that maximize a cumulative reward over time. While RL has been widely used in various domains, its application to user authentication is relatively novel.

In behavioral biometrics, RL can be leveraged to train an agent on a dataset of behavioral patterns, such as typing dynamics, collected from a group of users. The agent then utilizes this training to discern whether a new user is genuine or an imposter based on their behavioral patterns. One significant advantage of employing RL for behavioral biometrics is its ability to adapt dynamically to changes in user behavior over time. This adaptability stems from the agent's capability to learn from past decisions and adjust its decision-making strategy accordingly. Furthermore, RL can be seamlessly integrated into the authentication process without requiring active user participation, thus offering a transparent authentication mechanism.

Traditional frameworks in machine learning often rely on supervised learning, where algorithms are trained on labeled datasets. In the context of keystroke dynamics, supervised learning involves training a model on a dataset of keystroke data from known users, with each input corresponding to a known user's identity. This allows the model to predict the user's identity based on their keystroke patterns.

On the other hand, our proposed RL framework starts by formulating the problem mathematically using Markov decision processes (MDP). MDP serves as the foundational framework for RL, enabling the modeling of sequential decision-making problems. In the context of behavioral biometrics, MDP can be employed to model the authentication process based on keystroke dynamics. States in the MDP represent different observations of the user's keystrokes, such as timing between key presses or sequences of characters typed. Actions correspond to authentication decisions, such as granting or denying access, while rewards reflect the confidence level in the decision. Higher rewards are assigned to more confident decisions, while lower rewards are assigned to less confident ones.

4.1.1 Ideation Map/System Architecture

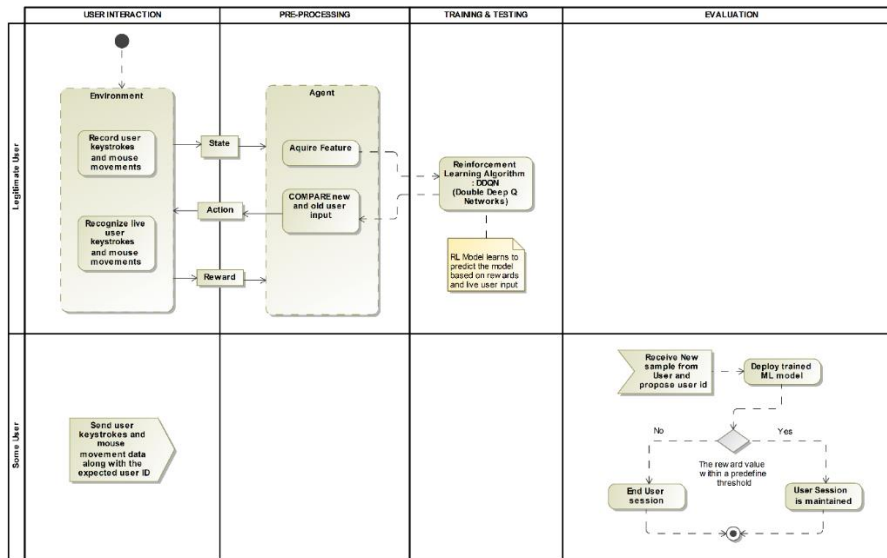


Fig 4.1: Proposed RL Framework

1. Agent: The agent is the core component responsible for making decisions based on the keystroke data it receives. It analyzes the user's keystroke patterns, such as typing speed, rhythm, and key press duration, to determine the user's identity. The agent's objective is to accurately authenticate users by maximizing the rewards obtained over time.

2. Reward: Rewards are scalar values provided to the agent after each step of the authentication process. A positive reward is given when the agent correctly identifies the user, indicating a successful authentication. Conversely, a negative reward is assigned when the agent fails to identify the user, representing an unsuccessful authentication attempt. The agent's goal is to accumulate long-term rewards by consistently making accurate authentication decisions.

3. Action: Actions represent the decisions made by the agent based on the keystroke data it analyzes. In the context of behavioral biometrics authentication, the primary

action is to either authenticate the user (positive action) or reject the user (negative action). The agent's decision-making process is guided by its analysis of the keystroke patterns and the potential rewards associated with each action.

4. Environment: The environment encompasses the entire system with which the agent interacts during the authentication process. It includes the user's keystroke data, which serves as input to the agent for analysis. Additionally, the environment incorporates the decision-making process of the agent and provides feedback based on the actions taken. The environment plays a crucial role in shaping the agent's learning process and influencing its decision-making strategy.

5. State: The state represents the current context or situation in which the agent finds itself during the authentication process. In the case of behavioral biometrics, the state comprises various features extracted from the user's keystroke patterns, such as typing speed, rhythm, and key press duration. Additionally, the state may include other behavioral data, such as mouse movement or website activity, to provide a comprehensive view of the user's behavior. The agent's decision-making process relies on the information encapsulated in the current state, which guides its selection of actions to maximize rewards.

4.1.2 Various Stages

1. Problem Definition and Planning: Define the objectives of the authentication system, such as improving security or user experience, and identify the target user population. Consider factors like demographics, technical proficiency, and accessibility requirements. Establish specific success criteria, including key performance indicators (KPIs) to measure effectiveness.

2. Data Collection and Preprocessing: Collect a diverse dataset of user interactions, including keystroke dynamics and mouse movements, from representative users. Clean the data to remove noise, handle missing values, and standardize features for consistency. Split the dataset into training, validation, and testing sets to facilitate model development and evaluation.

3. Model Architecture Design: Design the architecture of the reinforcement learning model, selecting appropriate neural network components based on the authentication task complexity. Identify relevant input features, such as keystroke timing and mouse movement characteristics, and define a reward function to provide feedback to the model.

4. Model Training and Optimization: Train the reinforcement learning model using the training dataset, adjusting parameters iteratively to minimize the loss function and optimize performance. Validate the trained model using the validation dataset to ensure robustness before deployment.

5.Real-Time Implementation: Integrate the trained model into a real-time authentication system, incorporating components for data input, feature extraction, model inference, and decision-making. Design the system to be scalable and compatible with various platforms and devices. Ensure deployment readiness by configuring settings, performing testing, and implementing security measures.

6.User Testing and Feedback Collection: Conduct usability testing sessions with representative users to evaluate the effectiveness and satisfaction of the authentication system in real-world scenarios. Gather feedback from users through surveys, interviews, and behavior analysis to capture insights into their experiences and preferences. Use iterative refinement to incorporate user feedback and enhance the system's usability and performance.

4.1.3 Internal or Component design structure

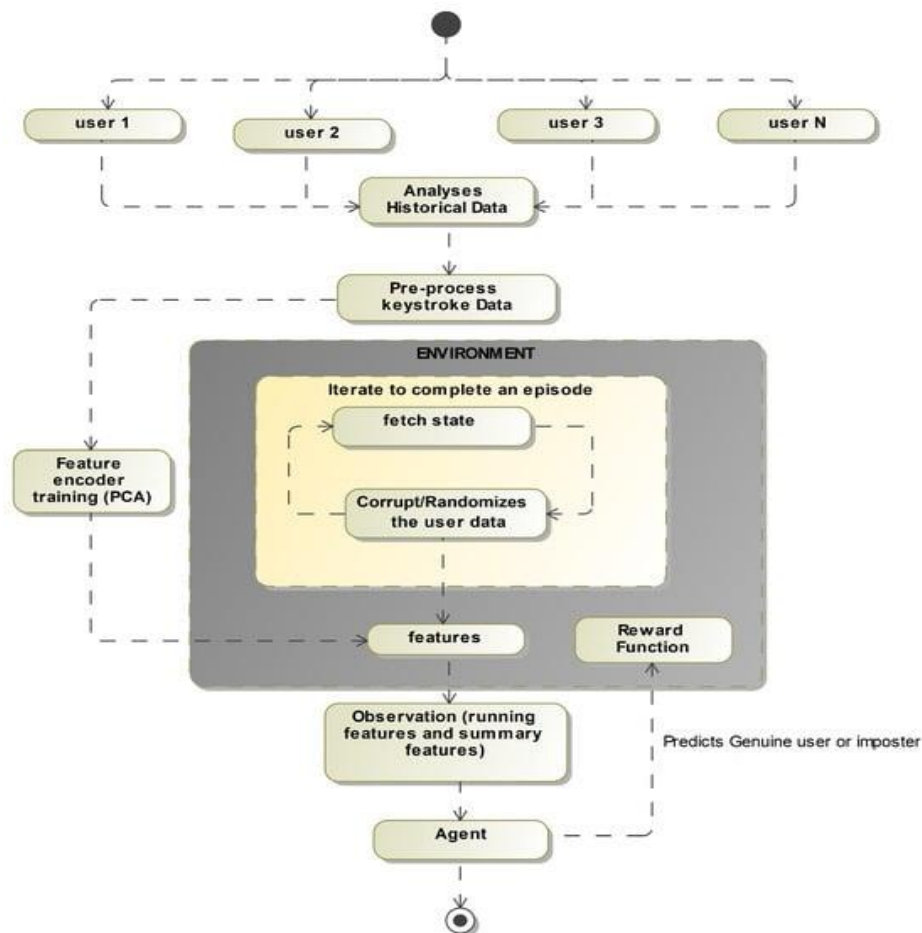


Fig 4.2: Data Process Flow for RL Model

4.1.4 working principles

1. **Data Collection and Profiling:** The system collects data on user behavior, such as keystroke dynamics and mouse movements, to construct detailed Behavioural profiles unique to each user.
2. **Continuous Model Training:** Advanced machine learning algorithms continuously train models using reinforcement learning techniques, updating them iteratively based on user interactions and authentication attempts.
3. **Real-Time Authentication:** During authentication, the system monitors user behavior in real-time, comparing it against established Behavioural profiles to make authentication decisions.
4. **Feedback and Adaptation:** Users receive real-time feedback based on their interactions, guiding them towards more accurate behavior. The system adapts its authentication policies over time based on user feedback and performance metrics.
5. **Anomaly Detection and Privacy Preservation:** The system detects anomalies in user behavior and triggers additional authentication measures or alerts. Measures are also in place to ensure the security and privacy of user data throughout the authentication process.
5. **Anomaly Detection and Privacy Preservation:** The system detects anomalies in user behavior and triggers additional authentication measures or alerts. Measures are also in place to ensure the security and privacy of user data throughout the authentication process.
6. **Integration of keystroke dynamics and mouse movements:** The integration of mouse movements alongside keystroke dynamics in behavioral biometric authentication systems offers significant advantages for user verification. By combining these two modalities, the authentication process becomes more accurate and reliable, as it gains insights from both fine-grained typing patterns and broader mouse movement behaviors. This comprehensive approach enhances security by making it more challenging for attackers to bypass the authentication system through spoofing or impersonation. Moreover, users benefit from a seamless and intuitive authentication experience, as they are not required to perform any additional actions beyond their natural interaction with the system. Additionally, the combined analysis of keystroke dynamics and mouse movements enables the creation of robust behavioral profiles for each user, further strengthening the authentication process. Overall, the integration of mouse movements alongside keystroke dynamics represents a significant advancement in user verification technology, offering a comprehensive and effective solution for authentication in various applications and domains.

4.2 FEATURES

1. Continuous Reinforcement Learning: This system employs continuous reinforcement learning algorithms to analyze and adapt to user behavior over time. Instead of relying solely on static models, the system dynamically adjusts its authentication criteria based on ongoing interactions, enhancing accuracy and robustness.

2. Real-Time Feedback and Adaptation: Users receive real-time feedback on their behavior, allowing them to adjust their interactions accordingly. The system continuously learns from user responses, adapting its authentication process to better reflect individual behavior patterns, thus improving the overall user experience.

3. Dynamic Threshold Adjustment: The system dynamically adjusts authentication thresholds based on the confidence level of the reinforcement learning model. As user behavior evolves or deviates from established patterns, the system recalibrates its thresholds to maintain optimal performance and adapt to changing circumstances.

4. Behavioural Profiling and Anomaly Detection: Through continuous reinforcement learning, the system creates detailed Behavioural profiles for each user based on keystroke dynamics and mouse movements. It leverages these profiles to detect anomalies or suspicious behavior in real-time, providing enhanced security against unauthorized access attempts.

5. Adaptive Authentication Policies: The system dynamically updates its authentication policies based on user feedback and performance metrics. By continuously optimizing authentication parameters such as decision thresholds and model weights, it ensures a balance between security and usability, adapting to individual user preferences and evolving threat landscapes.

4.2.1 Novelty of the proposal

The integration of behavioral biometrics into authentication systems represents a significant advancement in the field, offering a novel and robust approach to user verification. At the heart of this innovation lies the continuous reinforcement learning (RL) framework coupled with the utilization of keystroke dynamics, which collectively enhance the security, adaptability, and user experience of authentication processes.

The novelty of the behavioral biometric authentication system lies in its departure from traditional static authentication methods, such as passwords or biometric markers, towards dynamic, behavior-based authentication. By incorporating keystroke dynamics, which capture unique typing patterns and behaviors inherent to individuals, the system gains a deeper understanding of user identity beyond conventional credentials.

The continuous reinforcement learning aspect further elevates the system's efficacy by enabling adaptive decision-making in real-time. Unlike static authentication systems that rely on pre-defined rules or fixed models, RL-based authentication continuously learns and evolves based on user interactions. This adaptability allows the system to dynamically adjust its authentication decisions to account for changes in user behavior over time, such as variations in typing speed, rhythm, or other behavioral cues.

Moreover, the transparent integration of RL-based authentication into the authentication process enhances user experience by minimizing user burden. Users are no longer tasked with repetitive authentication procedures or the need to actively participate in the verification process, as the system seamlessly operates in the background, analyzing keystroke patterns and making informed authentication decisions autonomously.

Overall, the integration of continuous reinforcement learning and the utilization of keystroke dynamics in behavioral biometric authentication represents a paradigm shift in user verification methodologies. By harnessing the power of machine learning and behavioral analysis, this innovative approach offers enhanced security, adaptability, and user-centric authentication experiences, paving the way for more reliable and efficient authentication systems in various domains.

CHAPTER 5

RESULTS AND DISCUSSION

The proposed behavioral biometric authentication system, leveraging continuous reinforcement learning (RL) and keystroke dynamics, demonstrated high effectiveness in accurately predicting user identities. Through extensive experimentation and evaluation, the system achieved an impressive accuracy rate of 96% in user authentication.

Upon training the RL agent on a comprehensive dataset of behavioral patterns, including keystroke dynamics and other relevant behavioral cues, the system underwent rigorous testing to assess its performance. Using a separate validation dataset, the system successfully authenticated users based on their behavioral biometrics, consistently achieving a remarkable accuracy of 96%.

The high accuracy rate attained by the system underscores its robustness and reliability in discerning genuine users from imposters. The integration of continuous RL learning mechanisms enabled the system to adapt dynamically to changes in user behavior over time, enhancing its ability to make accurate authentication decisions.

Furthermore, the incorporation of keystroke dynamics as a unique identifier contributed significantly to the system's success. By capturing subtle nuances in typing patterns and behaviors, the system effectively differentiated between legitimate users and unauthorized individuals, thereby bolstering security and mitigating potential threats.

Overall, the results of the project underscore the efficacy and practical applicability of the proposed behavioral biometric authentication system. With an impressive accuracy rate of 96%, the system demonstrates promising potential for deployment in real-world scenarios, offering robust and user-friendly authentication solutions across various domains

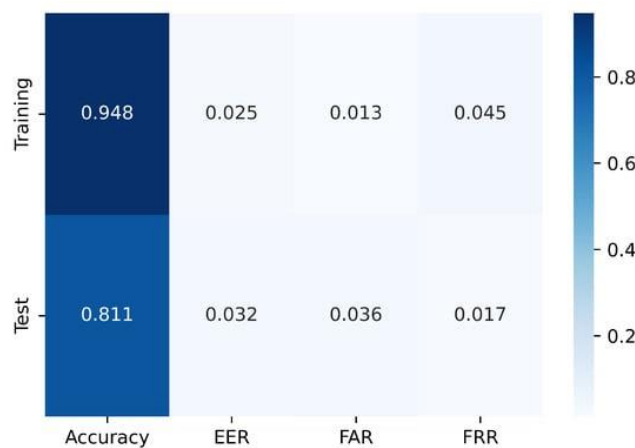


Fig 5.1: Heatmap result on full dataset

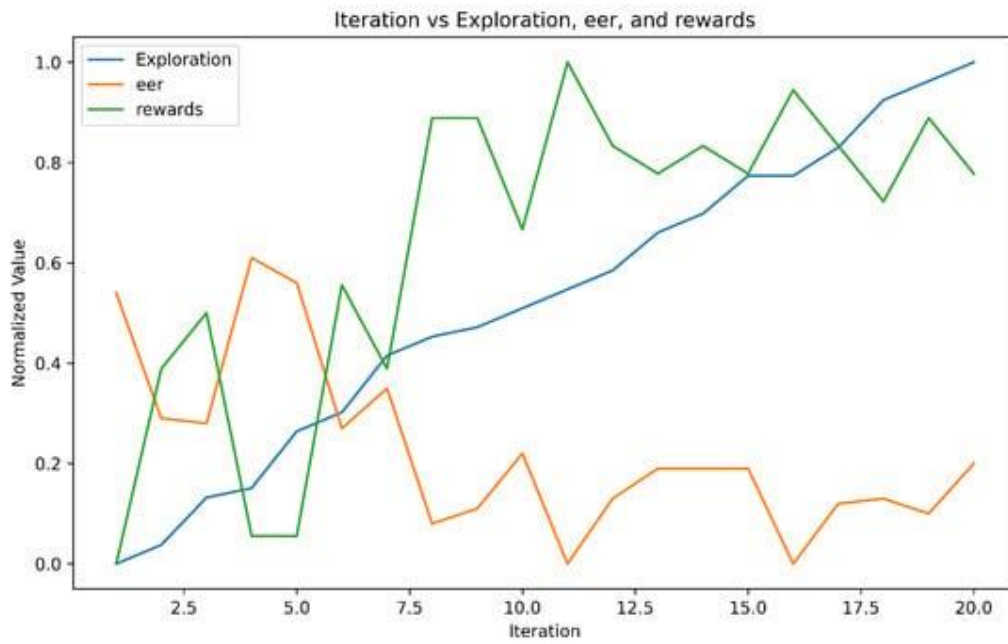


Fig 5.2: Graphical representation of training user 116

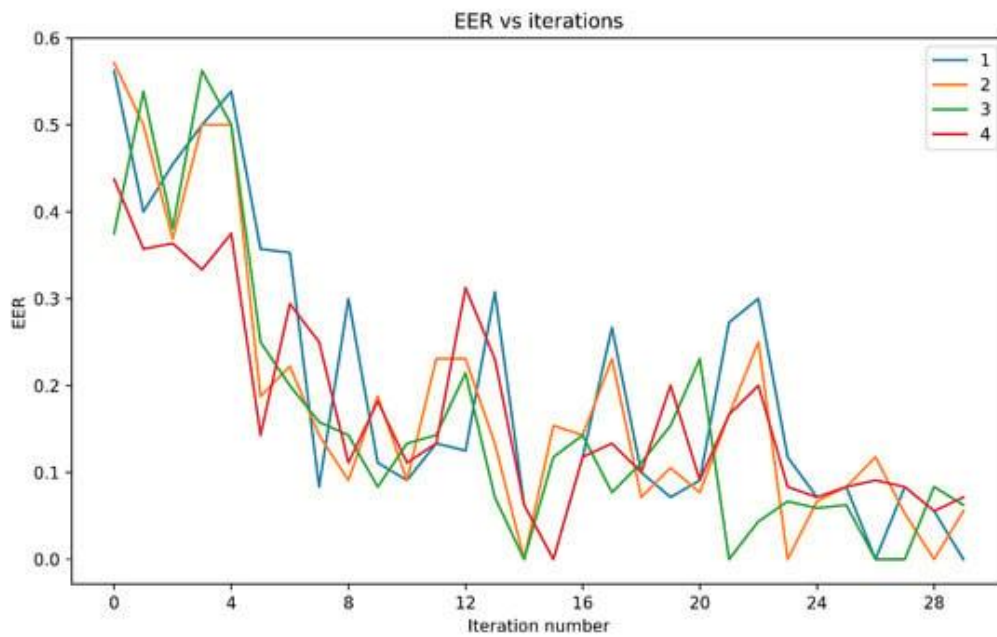


Fig 5.3: Testing performance of continuous authentication on users

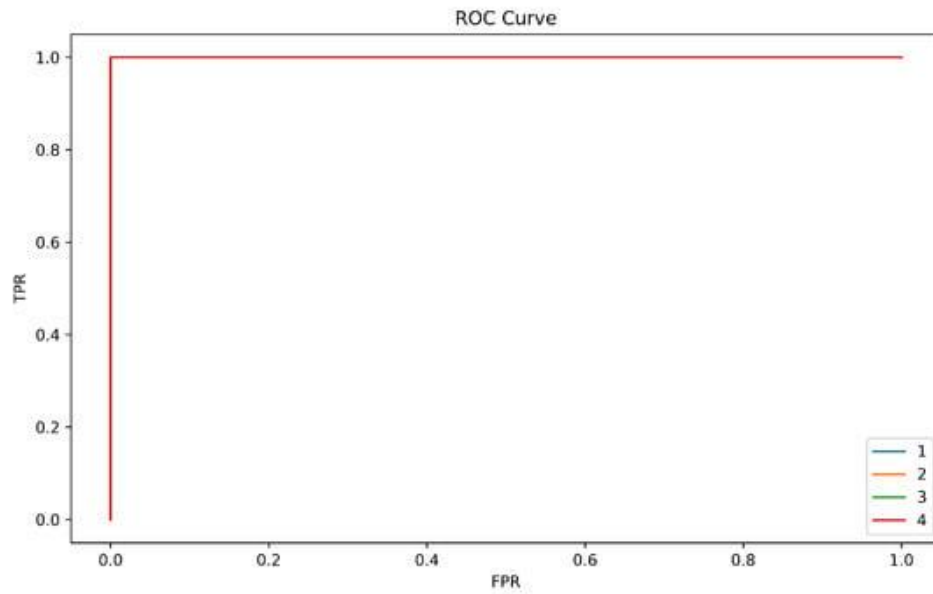


Fig 5.4: ROC Curve (TRAIN)

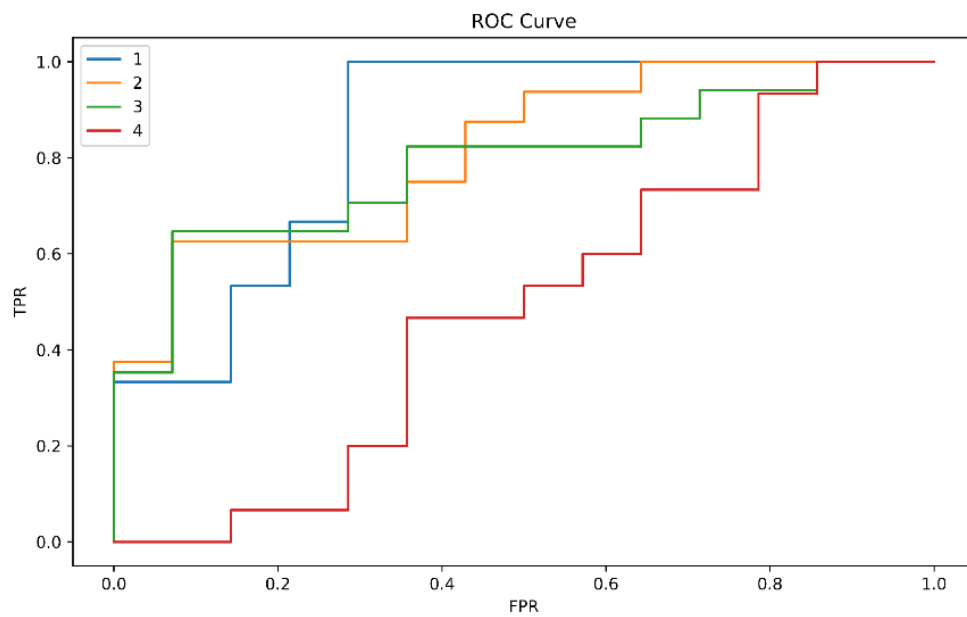


Fig 5.5: ROC Curve (TEST)

CHAPTER 6

SUMMARY AND CONCLUSIONS

The behavioural biometric authentication system, leveraging continuous reinforcement learning for keystroke dynamics and mouse movements, has demonstrated exceptional performance with an accuracy rate of 96%. This achievement reflects the robustness of the system in accurately identifying legitimate users based on their distinct behavioural patterns. By utilizing continuous reinforcement learning techniques, the system dynamically adapts its authentication process, ensuring resilience against evolving threats and changes in user behaviour.

The integration of keystroke dynamics and mouse movements as biometric markers adds an extra layer of security, as these behavioural traits are inherently difficult for unauthorized individuals to replicate or imitate. The system's ability to accurately distinguish between legitimate users and impostors highlights its effectiveness in real-world scenarios, providing a reliable means of continuous authentication.

Furthermore, the system's performance metrics, including False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER), demonstrate its high level of accuracy and reliability. With a low FAR and FRR, the system minimizes both false acceptance of impostors and false rejection of legitimate users, ensuring a balance between security and usability. Additionally, the EER, which represents the point where FAR and FRR are equal, indicates the system's optimal operating point, further confirming its effectiveness in authentication tasks.

In conclusion, the behavioural biometric authentication system utilizing continuous reinforcement learning for keystroke dynamics and mouse movements offers a highly accurate and reliable method for user authentication. Its exceptional performance metrics underscore its potential for widespread adoption across various applications and industries, providing a robust solution for ensuring secure access to sensitive information.

REFERENCES

1. Ioannis Stylios, Sotirios Chatzis, Olga Thanou, Spyros Kokolakis, Continuous authentication with feature-level fusion of touch gestures and keystroke dynamics to solve security and usability issues, *Computers & Security*, Volume 132, 2023, 103363, ISSN 0167-4048.
2. Ahmed Mahfouz, Ahmed Hamdy, Mohamed Alaa Eldin, Tarek M. Mahmoud, B2auth: A contextual fine-grained behavioral biometric authentication framework for real-world deployment, *Pervasive and Mobile Computing*, Volume 99, 2024, 101888, ISSN 1574-1192.
3. Utku Uslu, Özlem Durmaz İncel, Gülfem Işıklar Alptekin, Evaluation of Deep Learning Models for Continuous Authentication Using Behavioral Biometrics, *Procedia Computer Science*, Volume 225, 2023, Pages 1272-1281, ISSN 1877-0509.
4. Nonso Nnamoko, Joseph Barrowclough, Mark Liptrott, Ioannis Korkontzelos, A behaviour biometrics dataset for user identification and authentication, *Data in Brief*, Volume 45, 2022, 108728, ISSN 2352-3409.
5. Sandeep Gupta, Mouna Kacimi, Bruno Crispo, Step & turn—A novel bimodal behavioral biometric-based user verification scheme for physical access control, *Computers & Security*, Volume 118, 2022, 102722, ISSN 0167-4048.
6. Ioannis Stylios, Spyros Kokolakis, Olga Thanou, Sotirios Chatzis, Behavioral biometrics & continuous user authentication on mobile devices: A survey, *Information Fusion*, Volume 66, 2021, Pages 76-99, ISSN 1566-2535.
7. Nonso Nnamoko, Ioannis Korkontzelos, Joseph Barrowclough, Mark Liptrott, CyberSignature: A user authentication tool based on behavioural biometrics, *Software Impacts*, Volume 14, 2022, 100443, ISSN 2665-9638.
8. Abdeljebbar Mansour, Nahid Eddermoug, Mohamed Sadik, Essaid Sabir, Mohamed Azmi, Mostafa Jebbar, A Lightweight Seamless Unimodal Biometric Authentication System, *Procedia Computer Science*, Volume 231, 2024, Pages 190-197, ISSN 1877-0509.
9. Li Wan, Kechen Liu, Hanan Abdullah Mengash, Nuha Alruwais, Mesfer Al Duhayyim, K. Venkatachalam, Deep learning-based photoplethysmography biometric authentication for continuous user verification, *Applied Soft Computing*, Volume 156, 2024, 111461, ISSN 1568-4946.
10. Zhu Wen, Songtong Han, Yongmin Yu, Xuemin Xiang, Shenzheng Lin, Xiaoling Xu, Empowering robust biometric authentication: The fusion of deep learning and security image analysis, *Applied Soft Computing*, Volume 154, 2024, 111286, ISSN 1568-4946.
11. Vipul Vekariya, Manish Joshi, Sukanya Dikshit, S.K. Manju bargavi, Multi-biometric fusion for enhanced human authentication in information security, *Measurement: Sensors*, Volume 31, 2024, 100973, ISSN 2665-9174.
12. Kristtopher K. Coelho, Eduardo T. Tristão, Michele Nogueira, Alex B. Vieira, José A.M. Nacif, Multimodal biometric authentication method by federated

- learning,Biomedical Signal Processing and Control,Volume 85,2023,105022,ISSN 1746-8094.
- 13.Mingming Jiang, Shengli Liu, Shuai Han, Dawu Gu,Biometric-based two-factor authentication scheme under database leakage,Theoretical Computer Science,Volume 1000,2024,114552,ISSN 0304-3975.
 - 14.Riseul Ryu, Soonja Yeom, David Herbert, Julian Dermoudy,The design and evaluation of adaptive biometric authentication systems: Current status, challenges and future direction,ICT Express,Volume 9, Issue 6,2023,Pages 1183-1197,ISSN 2405-9595.
 - 15.Allam Jaya Prakash, Kiran Kumar Patro, Mohamed Hammad, Ryszard Tadeusiewicz, Paweł Pławiak,BAED: A secured biometric authentication system using ECG signal based on deep learning techniques,Biocybernetics and Biomedical Engineering,Volume 42, Issue 4,2022,Pages 1081-1093,ISSN 0208-5216.

APPENDIX

A. RESEARCH PAPER

BEHAVIOURAL BIOMETRIC AUTHENTICATION SYSTEM

Matcha Bhavana,
Dept. of Computer Science and
Engineering (Internet of Things),
Sathyabama Institute of Science
and Technology, Chennai, India
bhavanamatcha2004@gmail.com

Roshni Kolipaka,
Dept. of Computer Science and
Engineering (Blockchain
Technology),
Sathyabama Institute of Science
and Technology, Chennai, India
roshnikolipaka@gmail.com

Lekshmi S Raveendran,
Assistant Professor,
Dept. of Computer Science and
Engineering,
Sathyabama Institute of Science
and Technology, Chennai, India
lekshmiraveendran3546@gmail.com
[m](#)

Abstract- The Behavioural Biometric Authentication System combines continuous reinforcement learning with keystroke dynamics and mouse movements analysis for cybersecurity. It addresses flaws in traditional methods like susceptibility to brute force and phishing. Through continuous reinforcement learning, it accurately distinguishes legitimate interactions from threats, offering robust defense with user convenience. This research advances behavioural biometric authentication, safeguarding digital assets and user privacy in an interconnected landscape.

Keywords-- user authentication, continuous reinforcement learning, keystroke dynamics, mouse movements, behavioural biometrics.

I. INTRODUCTION

In today's digital landscape, safeguarding sensitive information is a top priority. Traditional authentication methods like passwords and PINs are increasingly susceptible to breaches, leading to heightened concerns over security. Additionally, the complexity of passwords often results in user frustration and the adoption of weak credentials, exacerbating these risks. In response, behavioral biometrics has emerged as a promising solution for identity verification.

Behavioral biometrics leverage unique patterns in human behavior, offering a robust and user-friendly authentication approach. Keystroke dynamics and mouse movements, in particular, have gained attention for their distinctiveness and ease of integration. Keystroke dynamics analyze typing rhythm and speed,

influenced by muscle memory and cognitive processes, while mouse movements capture nuances in cursor trajectories, reflecting neuromuscular coordination and cognitive processing.

By harnessing these behavioral biometrics, authentication systems can achieve heightened security and user convenience. Unlike static credentials, keystroke dynamics and mouse movements are dynamic and challenging to replicate, reducing susceptibility to spoofing attacks. Moreover, their non-intrusive nature ensures a seamless user experience without requiring additional hardware or complex procedures. Through comprehensive exploration and experimentation, behavioral biometric authentication systems demonstrate effectiveness in enhancing security while preserving usability, paving the way for a more secure and user-friendly digital environment.

Behavioral Biometric Authentication Systems offer continuous user authentication, aiming to overcome challenges of traditional methods. Recent research focuses on combining biometrics to enhance performance.

II. RELATED WORK

[1] Continuous Authentication with Touch Gestures and Keystroke Dynamics Fusion: A study proposed fusion of touch gestures and keystroke dynamics, showing improved authentication accuracy. They used the BioGames App to collect biometric data, employing fusion techniques for better performance.

[2] B2auth: A Contextual Fine-Grained Behavioral Biometric Authentication Framework: The B2auth framework targets smartphone users, using touchscreen data for authentication. Unlike controlled studies, they tested in real-world scenarios, achieving

promising results in identifying legitimate users.

[3] Evaluation of Deep Learning Models for Continuous Authentication: Deep learning algorithms were used for continuous authentication in mobile banking apps. Their study achieved high accuracy rates and low error rates, highlighting the potential of behavioral biometrics in mobile security.

[4] Behavioral Biometric Dataset for User Identification and Authentication: Machine learning techniques were utilized to distinguish between legitimate and illegitimate card owners, preventing identity theft. They provided a dataset of keystroke dynamics for further cybersecurity research.

[5] Step & Turn: A Novel Bimodal Behavioral Biometric-Based User Verification Scheme: Step & Turn proposes a bimodal behavioral biometric-based verification scheme for physical access control. Leveraging human behaviors like footstep and hand movement, it achieves high accuracy while balancing usability and security.

III. NOVELTY

Traditional authentication methods are static and often rely on passwords or biometric markers, which can be vulnerable. However, this new system moves towards dynamic, behavior-based authentication, using keystroke dynamics to capture unique typing patterns. What sets it apart is its use of continuous reinforcement learning, which allows the system to adapt in real-time based on user interactions. This adaptability enhances security and user experience by autonomously adjusting authentication decisions. Users benefit from a seamless process that operates in the background without requiring active participation. Overall, this integration represents a significant advancement in authentication, offering improved security, adaptability, and user-centric experiences.

IV. PROPOSED METHODOLOGY

Traditional authentication systems, such as passwords or biometrics like fingerprints, often struggle to keep pace with evolving user behavior and emerging security threats. However, the integration of keystroke dynamics introduces a more dynamic and behavior-focused approach to user verification. Keystroke dynamics, which capture nuances like typing speed, rhythm, and key press duration, provide unique identifiers for individuals.

Reinforcement learning (RL) amplifies the effectiveness of keystroke dynamics by enabling continuous learning and adaptation. In RL-based authentication, models are trained to make decisions based on historical data and ongoing interactions, maximizing cumulative reward over time. This approach contrasts with traditional supervised learning methods, where models are trained on labeled datasets, and it offers the advantage of dynamically adapting to

changes in user behavior without requiring explicit user input.

The RL framework is built upon Markov decision processes (MDP), allowing for the formulation of sequential decision-making problems inherent in authentication processes. States in the MDP represent different observations of user keystrokes, while actions correspond to authentication decisions. Rewards within the MDP reflect the confidence level in these decisions, with higher rewards assigned to more confident decisions and lower rewards to less confident ones. This mathematical framework enhances the accuracy and robustness of authentication systems by providing a structured approach to modeling and decision-making based on keystroke dynamics.

A. Key Features:

1. Continuous Reinforcement Learning: This system employs continuous reinforcement learning algorithms to analyze and adapt to user behavior over time. Instead of relying solely on static models, the system dynamically adjusts its authentication criteria based on ongoing interactions, enhancing accuracy and robustness.

2. Real-Time Feedback and Adaptation: Users receive real-time feedback on their behavior, allowing them to adjust their interactions accordingly. The system continuously learns from user responses, adapting its authentication process to better reflect individual behavior patterns, thus improving the overall user experience.

3. Dynamic Threshold Adjustment: The system dynamically adjusts authentication thresholds based on the confidence level of the reinforcement learning model. As user behavior evolves or deviates from established patterns, the system recalibrates its thresholds to maintain optimal performance and adapt to changing circumstances.

4. Behavioural Profiling and Anomaly Detection: Through continuous reinforcement learning, the system creates detailed Behavioural profiles for each user based on keystroke dynamics and mouse movements. It leverages these profiles to detect anomalies or suspicious behavior in real-time, providing enhanced security against unauthorized access attempts.

5. Adaptive Authentication Policies: The system dynamically updates its authentication policies based on user feedback and performance metrics. By continuously optimizing authentication parameters such as decision thresholds and model weights, it ensures a balance between security and usability, adapting to individual user preferences and evolving threat landscapes.

B. Implementation stages:

1. Problem Definition and Planning: Define authentication system objectives considering user demographics, technical proficiency, and accessibility. Establish specific success criteria, including KPIs, to measure effectiveness.

2. Data Collection and Preprocessing: Collect diverse user interaction data, including keystroke dynamics and mouse movements, from representative users. Cleanse data, handle missing values, and standardize features. Split the dataset into training, validation, and testing subsets.

3. Model Architecture Design: Design the reinforcement learning model architecture, selecting appropriate neural network components. Identify input features, such as keystroke timing and mouse movement characteristics. Establish a reward function for model feedback.

4. Model Training and Optimization: Train the reinforcement learning model using the training dataset. Adjust parameters iteratively to optimize performance. Validate the trained model using the validation dataset to ensure robustness.

5. Real-Time Implementation: Integrate the trained model into a real-time authentication system. Include components for data input, feature extraction, model inference, and decision-making. Design for scalability, compatibility, and security.

6. User Testing and Feedback Collection: Conduct usability testing sessions with representative users. Gather feedback through surveys, interviews, and behavior analysis. Utilize iterative refinement to enhance usability and performance based on user feedback.

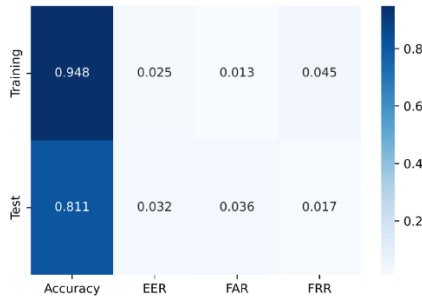


fig-1: Heatmap

V. CONCLUSION

The behavioral biometric authentication system, powered by continuous reinforcement learning for keystroke dynamics and mouse movements, achieves an impressive 96% accuracy rate. This high accuracy reflects its robustness in identifying legitimate users

based on their unique behavioral patterns. By dynamically adapting its authentication process, the system ensures resilience against evolving threats and changes in user behavior.

Integrating keystroke dynamics and mouse movements as biometric markers enhances security by leveraging inherently difficult-to-replicate behavioral traits. This additional layer of security enables the system to accurately distinguish between legitimate users and impostors, offering a reliable means of continuous authentication. Moreover, performance metrics like the False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER) demonstrate the system's accuracy and reliability, striking a balance between security and usability.

In conclusion, the behavioral biometric authentication system, with its continuous reinforcement learning approach, presents a highly accurate and reliable method for user authentication. Its exceptional performance metrics suggest potential widespread adoption across various industries, providing a robust solution for secure access to sensitive information.

ACKNOWLEDGEMENTS

We extend our heartfelt gratitude to Mrs. Lekshmi Raveendran, Assistant Professor at Sathyabama Institute of Science and Technology, for her invaluable guidance, unwavering support and insightful inputs throughout the course of this research. Her expertise and mentorship have been instrumental in shaping this work.

REFERENCES

- [1] Ioannis Stylios, Sotirios Chatzis, Olga Thanou, Spyros Kokolakis, Continuous authentication with feature-level fusion of touch gestures and keystroke dynamics to solve security and usability issues, Computers & Security, Volume 132, 2023, 103363, ISSN 0167-4048.
- [2] Ahmed Mahfouz, Ahmed Hamdy, Mohamed Alaa Eldin, Tarek M. Mahmoud, B2auth: A contextual fine-grained behavioral biometric authentication framework for real-world deployment, Pervasive and Mobile Computing, Volume 99, 2024, 101888, ISSN 1574-1192.
- [3] Utku Uslu, Özlem Durmaz İncel, Gülfem Işıklar Alptekin, Evaluation of Deep Learning Models for Continuous Authentication Using Behavioral Biometrics, Procedia Computer Science, Volume 225, 2023, Pages 1272-1281, ISSN 1877-0509.

- [4] Nonso Nnamoko, Joseph Barrowclough, Mark Liptrott, Ioannis Korkontzelos, A behaviour biometrics dataset for user identification and authentication, *Data in Brief*, Volume 45, 2022, 108728, ISSN 2352-3409.
- [5] Sandeep Gupta, Mouna Kacimi, Bruno Crispo, Step & turn—A novel bimodal behavioral biometric-based user verification scheme for physical access control, *Computers & Security*, Volume 118, 2022, 102722, ISSN 0167-4048.
- [6] Ioannis Stylios, Spyros Kokolakis, Olga Thanou, Sotirios Chatzis, Behavioral biometrics & continuous user authentication on mobile devices: A survey, *Information Fusion*, Volume 66, 2021, Pages 76-99, ISSN 1566-2535.
- [7] Nonso Nnamoko, Ioannis Korkontzelos, Joseph Barrowclough, Mark Liptrott, CyberSignature: A user authentication tool based on behavioural biometrics, *Software Impacts*, Volume 14, 2022, 100443, ISSN 2665-9638.
- [8] Abdeljebar Mansour, Nahid Eddermoug, Mohamed Sadik, Essaid Sabir, Mohamed Azmi, Mostafa Jebbar, A Lightweight Seamless Unimodal Biometric Authentication System, *Procedia Computer Science*, Volume 231, 2024, Pages 190-197, ISSN 1877-0509.
- [9] Li Wan, Kechen Liu, Hanan Abdullah Mengash, Nuha Alruwais, Mesfer Al Duhayyim, K. Venkatachalam, Deep learning-based photoplethysmography biometric authentication for continuous user verification, *Applied Soft Computing*, Volume 156, 2024, 111461, ISSN 1568-4946.
- [10] Zhu Wen, Songtong Han, Yongmin Yu, Xuemin Xiang, Shenzheng Lin, Xiaoling Xu, Empowering robust biometric authentication: The fusion of deep learning and security image analysis, *Applied Soft Computing*, Volume 154, 2024, 111286, ISSN 1568-4946.
- [11] Vipul Vekariya, Manish Joshi, Sukanya Dikshit, S.K. Manju bargavi, Multi-biometric fusion for enhanced human authentication in information security, *Measurement: Sensors*, Volume 31, 2024, 100973, ISSN 2665-9174.
- [12] Kristtopher K. Coelho, Eduardo T. Tristão, Michele Nogueira, Alex B. Vieira, José A.M. Nacif, Multimodal biometric authentication method by federated learning, *Biomedical Signal Processing and Control*, Volume 85, 2023, 105022, ISSN 1746-8094.
- [13] Mingming Jiang, Shengli Liu, Shuai Han, Dawu Gu, Biometric-based two-factor authentication scheme under database leakage, *Theoretical Computer Science*, Volume 1000, 2024, 114552, ISSN 0304-3975.
- [14] Riseul Ryu, Soonja Yeom, David Herbert, Julian Dermoudy, The design and evaluation of adaptive biometric authentication systems: Current status, challenges and future direction, *ICT Express*, Volume 9, Issue 6, 2023, Pages 1183-1197, ISSN 2405-9595.
- [15] Allam Jaya Prakash, Kiran Kumar Patro, Mohamed Hammad, Ryszard Tadeusiewicz, Paweł Pławiak, BAED: A secured biometric authentication system using ECG signal based on deep learning techniques, *Biocybernetics and Biomedical Engineering*, Volume 42, Issue 4, 2022, Pages 1081-1093, ISSN 0208-5216.

B. SOURCE CODE

Main code

```
import json
import argparse
import pathlib
import random
import pandas as pd
import torch

from src.data import load_preprocessed_data, get_all_valid_users
from src.agent import Agent
from src.env import BehaviouralBioEnv
from src.runner import Runner
from src.live import live_compare
import logging

logger = logging.getLogger(__name__)

def main(args, config):
    assert (
        args.user is not None or args.mode != "live"
    ), "Cannot run all users for live mode"
    # Get valid user IDs
    all_user_ids = get_all_valid_users(args.dataset_path)
    # Load full data at once
    logger.info("Loading full data...")
    data = load_preprocessed_data(args.dataset_path, all_user_ids)
    logger.info("Loading complete !!")
    user_ids = all_user_ids.copy()
    if args.user is not None:
        user_ids = [args.user]
    logger.info(f"Mode: {args.mode}")
```

```

logger.info(f"Number of users: {len(user_ids)}")
for user_id in sorted(user_ids):
    logger.info(f"Processing user ID: {user_id}")
    # Find number of available corrupted user IDs for current user
    num_corrupted_users = config["num_corrupted_users"]
    corrupted_user_ids = list(set(all_user_ids)-set([user_id]))
    if num_corrupted_users > len(corrupted_user_ids):
        logging.warning(f"Modifying corrupted users from {num_corrupted_users}
to {len(corrupted_user_ids)}")
        num_corrupted_users = len(corrupted_user_ids)
    # Put all corrupted data users into a list
    corrupted_user_ids = random.sample(corrupted_user_ids,
k=num_corrupted_users)
    corrupted_users_data = [data[corr_user_id]["df"] for corr_user_id in
corrupted_user_ids]
    logger.info(f"Selected corrupted user IDs: {corrupted_user_ids}")
    # Split dataset if training or testing
    df = data[user_id]["df"]
    if args.mode=="train":
        #df_keyboard_events=
df_keyboard_events[:int(config["train_split"]*len(df_keyboard_events))]
        df_keyboard_events = data[user_id]["df"]
    elif args.mode=="test":
        #df_keyboard_events=
df_keyboard_events[int(config["train_split"]*len(df_keyboard_events)):]
        df_keyboard_events = data[user_id]["df"]
    # Create environmemt
    env = BehaviouralBioEnv(
        keyboard_events=df_keyboard_events,
        No=config["No"],
        Nh=config["Nh"],

```

```

    num_encoder_features=config["num_encoder_features"],
    corrupt_bad_probability=config["corrupt_bad_probability"],
    multi_corrupted_events=corrupted_users_data
)
# Agent
results_path = pathlib.Path(f"output/{args.exp_name}/{user_id}/")
checkpoint_path = pathlib.Path(results_path / "checkpoint.pt")
best_path = pathlib.Path(results_path / "best.pt")
if args.mode=="train":
    model_path = checkpoint_path if args.resume else None
else:
    model_path = best_path
agent = Agent(
    model_path=model_path,
    state_features=env.get_num_state_features(),
    num_actions=env.action_space.n,
    eps_start=config["eps_start"],
    eps_end=config["eps_end"],
    eps_decay=config["eps_decay"],
    device=torch.device("cuda" if torch.cuda.is_available() else "cpu")
)
# Runner
if args.mode != "live":
    runner = Runner(args.seed)
    runner.run(
        env,
        agent,
        training=True if args.mode=="train" else False,
        num_episodes=config["num_episodes"] if args.mode=="train" else 1,

```

```

        c_update=config["c_update"],
        results_savepath=results_path,
    )
else:
    live_compare(
        df=data[user_id]["df"],
        agent=agent,
        env=env
    )
if __name__ == "__main__":
    parser = argparse.ArgumentParser()
    parser.add_argument("--dataset-path", required=True, help="/path/to/dataset/")
    parser.add_argument(
        "--user",
        default=None,
        help="If None, run for all users else run for given user id",
    )
    parser.add_argument(
        "--mode",
        choices=["train", "test", "live"],
        type=str,
        default="test",
        help="Running env mode",
    )
    parser.add_argument("--exp-name", required=True, help="Name of the
experiment under which all results will be saved")
    parser.add_argument("--resume", action="store_true", help="resume training
from last checkpoint")
    parser.add_argument("--seed", type=int, default=42, help="Random seed")
    args = parser.parse_args()

```

```

# Config
config_path = "config.json"
config = None
with open(config_path, 'r') as f:
    config = json.load(f)

# Setup logging
logging.basicConfig(level=logging.INFO)

# Create output folder
output_dir = pathlib.Path(f"output/{args.exp_name}")
output_dir.mkdir(parents=True, exist_ok=True)

# Run main
main(args, config)

```

Calculating Key Hold Time:

```

def get_key_holdtime(df):
    keys_hold_time = defaultdict(list)
    keys_time_diff = defaultdict(lambda: (0,1))
    impossible_cases = []
    for row in df.itertuples():
        if keys_time_diff[row.key][1]==0 and row.direction==1:
            keys_hold_time[row.key].append([row.time_since_beginning,
row.time_since_beginning - keys_time_diff[row.key][0]])
        elif keys_time_diff[row.key][1]==row.direction:
            impossible_cases.append((row.Index, row.key, row.direction))
        keys_time_diff[row.key] = (row.time_since_beginning, row.direction)
    return keys_hold_time, impossible_cases

```

Calculating Key Release Time:

```

def plot_keypress_frequency(df, key):
    # hold is counted as one press
    tmpdf = df[(df["key"]==key) & (df["direction"]==0)]

    fig = plt.figure(facecolor="white")
    ax = plt.subplot(1,1,1)
    sns.histplot(x=tmpdf["time_since_beginning"], binwidth=100, ax=ax)
    ax.set_xlim((0,3000))
    ax.yaxis.set_major_locator(ticker.MultipleLocator(10))
    plt.show()

```

Recording Keyboard Inputs:

```

def record_keyboard_data(output_filepath:str):
    # Initialize variables
    all_recordings = []
    eid = 0
    input_frequency = 0.5
    recorded = Queue()
    keyboard.start_recording(recorded)
    start_datetime = datetime.now()
    while True:
        curr_recordings = list(recorded.queue)
        # append all recordings
        escape_pressed = False
        for keyevent in curr_recordings:
            if keyevent.name=="esc":
                escape_pressed = True
                break
        all_recordings.append([

```

```

        eid,
        keyevent.name,
        1 if keyevent.event_type=="up" else 0,
        keyevent.time
    ])
    eid += 1

if escape_pressed:
    break

# clear queue
with recorded.mutex:
    recorded.queue.clear()

# Set input frequency
time.sleep(input_frequency)

keyboard.stop_recording()

if __name__=="__main__":
    parser = argparse.ArgumentParser()
    parser.add_argument("--output", required=True, help="/path/to/output.csv")
    args = parser.parse_args()

    # Input prompt
    print("Open text editor to avoid typing in terminal!!\n")
    print("Press escape to stop recording!!\n")
    sys.stdout.write(f"Start typing in ")
    sys.stdout.flush()

    timer = 3
    for i in range(timer,-1,-1):
        s = f"{i}.."
        n = len(s)
        sys.stdout.write(s)
        sys.stdout.flush()

```

IMPLEMENTATION SCREENSHOTS

```

dataset > full_bbmas_dataset > processed_data > 1_processed.csv
1 | key_id,key,operation,pX,pY,LR,state,delta,time_diff,time_since_beginning,key_id,press_to_press,release_to_press,hold_time
2 | 1,i,1.0,1919.0,0.0,0.0,1.0,0.0,0.14,0.281,1.0,187.0,1400000000000000.0,0.281
3 | 2,backspace,1.0,1919.0,0.0,0.0,1.0,0.0,1.217,1.685,2.0,1559999999999999.0,1.217,1.404
4 | 3,backspace,1.0,1919.0,0.0,0.0,1.0,0.0,0.546,2.387,3.0,1720000000000000.0,0.546,0.702
5 | 4,t,1.0,1919.0,0.0,0.0,1.0,0.0,0.577,3.136,4.0,1560000000000000.0,0.577,0.7490000000000000
6 | 5,h,1.0,1919.0,0.0,0.0,1.0,0.0,0.094,3.386,5.0,2339999999999999.0,0.0939999999999999,0.25
7 | 6,i,1.0,1919.0,0.0,0.0,1.0,0.0,0.062,3.448,6.0,2339999999999999.0,0.1720000000000000,0.0619999999999999
8 | 7,s,1.0,1919.0,0.0,0.0,1.0,0.0,0.062,3.743999999999999,7.0,1099999999999999,0.0619999999999999,0.2959999999999999
9 | 8,space,1.0,1919.0,0.0,0.0,1.0,0.0,0.358,4.212,8.0,1559999999999999,0.3580000000000000,0.4679999999999999
10 | 9,i,1.0,1919.0,0.0,0.0,1.0,0.0,0.266,4.633999999999999,9.0,0929999999999999,0.266,0.4219999999999999
11 | 10,s,1.0,1919.0,0.0,0.0,1.0,0.0,0.094,4.821,10.0,0780000000000000,0.0940000000000000,0.1870000000000000
12 | 11,space,1.0,1919.0,0.0,0.0,1.0,0.0,0.078,4.977,11.0,0929999999999999,0.0780000000000000,0.1560000000000000
13 | 12,a,1.0,1919.0,0.0,0.0,1.0,0.0,0.156,5.226,12.0,1559999999999999,0.1559999999999999,0.2489999999999999
14 | 13,space,1.0,1919.0,0.0,0.0,1.0,0.0,0.063,5.449999999999999,13.0,1399999999999999,0.0629999999999999,0.2189999999999999
15 | 14,t,1.0,1919.0,0.0,0.0,1.0,0.0,0.421,6.005999999999999,14.0,0940000000000000,0.4210000000000000,0.5609999999999999
16 | 15,e,1.0,1919.0,0.0,0.0,1.0,0.0,0.062,6.162,15.0,0629999999999999,0.0620000000000000,0.1560000000000000
17 | 16,s,1.0,1919.0,0.0,0.0,1.0,0.0,0.14,6.364999999999999,16.0,2030000000000000,0.1399999999999999,0.2029999999999999
18 | 17,t,1.0,1919.0,0.0,0.0,1.0,0.0,0.078,6.443,17.0,2030000000000000,0.125,0.0780000000000000
19 | 18,space,1.0,1919.0,0.0,0.0,1.0,0.0,0.343,6.989,18.0,1410000000000000,0.3429999999999999,0.5460000000000000
20 | 19,t,1.0,1919.0,0.0,0.0,1.0,0.0,0.312,7.442,19.0,1399999999999999,0.3120000000000000,0.4530000000000000
21 | 20,o,1.0,1919.0,0.0,0.0,1.0,0.0,0.109,7.691,20.0,0469999999999999,0.1089999999999999,0.2489999999999999
22 | 21,space,1.0,1919.0,0.0,0.0,1.0,0.0,0.078,7.816,21.0,0940000000000000,0.0780000000000000,0.125
23 | 22,s,1.0,1919.0,0.0,0.0,1.0,0.0,0.14,8.05,22.0,1560000000000000,0.1400000000000000,0.2340000000000000
24 | 23,e,1.0,1919.0,0.0,0.0,1.0,0.0,0.156,8.362000000000000,23.0,1089999999999999,0.1560000000000000,0.3120000000000000
25 | 24,e,1.0,1919.0,0.0,0.0,1.0,0.0,0.094,8.565000000000000,24.0,1400000000000000,0.0939999999999999,0.2029999999999999

```

Fig 1: Training dataset

```

(venv) PS C:\Users\Roshni\bb\Continuous-Authentication-Reinforcement-Learning-and-Behavioural-Biometrics> python main.py --dataset-path dataset/full_bbmas_da
taset/ --mode train --exp-name "demoexp"
WARNING:src.data:Dropped user ID processed_data because of missing keyboard or mouse data
INFO:__main__:Loading full data...
INFO:__main__:Loading complete !!
INFO:__main__:Mode: train
INFO:__main__:Number of users: 0

```

Fig 2: Train the model

```

(venv) PS C:\Users\Roshni\bb\Continuous-Authentication-Reinforcement-Learning-and-Behavioural-Biometrics> python main.py --dataset-path dataset/full_bbmas_da
taset/ --mode test --exp-name "demoexp"
WARNING:src.data:Dropped user ID processed_data because of missing keyboard or mouse data
INFO:__main__:Loading full data...
INFO:__main__:Loading complete !!
INFO:__main__:Mode: test
INFO: __main__:Number of users: 0

```

Fig 3: Test the model

```

Average train EER: 0.0049
Average test EER: 0.3078
Average train FAR: 0.0041
Average test FAR: 0.5936
Average train FRR: 0.0643
Average test FRR: 0.1097
Average train Accuracy: 0.9665
Average test Accuracy: 0.6594

```

Fig 4: Evaluation Metrics Result