IJAICET, Vol. 1, Issue 1, July - September, 2026

AN ADAPTIVE RISK-BASED AUTHENTICATION FRAMEWORK USING BEHAVIORAL BIOMETRICS AND MACHINE LEARNING FOR CONTINUOUS USER VERIFICATION IN WEB APPLICATIONS

Mr. Ekele Olu [1]

Abstract- Authentication remains one of the most important security requirements in modern web applications. Traditional authentication methods, such as passwords and one-time passwords, verify users only during login and provide limited protection against threats such as session hijacking, credential theft, automated bots, and account takeover after authentication. As cyber threats continue to evolve, there is a growing need for intelligent systems that can continuously verify user identity throughout an active session without disrupting the user experience.This study presents an adaptive risk-based authentication framework that combines behavioural biometrics with machine learning for continuous user verification. The framework captures users' behavioural patterns, including mouse movements, keyboard activity, scrolling behaviour, click frequency, idle time, and session characteristics. These features are converted into numerical data and analysed using a Random Forest model to classify user sessions as either legitimate or suspicious. The model's predictions are then incorporated into a dynamic risk-scoring mechanism that supports adaptive security decisions.The system was developed using React for the client interface, NestJS for backend services, PostgreSQL with Prisma ORM for data management, and FastAPI for machine learning deployment. The microservice architecture allows efficient communication between behavioural data collection, feature extraction, machine learning prediction, and risk assessment while supporting future improvements without affecting the core system.The results demonstrate that combining multiple behavioural features provides more accurate contextual information than traditional authentication methods alone. Continuous behavioural monitoring improves fraud detection, reduces false authentication decisions, and enhances web application security through adaptive risk assessment. This study provides a practical framework that bridges the gap between behavioural authentication research and real-world web security applications while establishing a foundation for future research in deep learning, larger behavioural datasets, and real-time adaptive security systems.

Keywords: Behavioural Biometrics, Continuous Authentication, Machine Learning, Random Forest, Fraud Detection, Risk-Based Authentication, Web Security.

1. INTRODUCTION

1.1 Background of the Study

The increasing dependence on web applications for banking, healthcare, education, e-commerce, and government services has made user authentication a critical component of cybersecurity. Although conventional authentication methods such as passwords, one-time passwords (OTPs), and multi-factor authentication (MFA) provide an initial layer of protection, they authenticate users only at login and generally assume that the authenticated session remains secure thereafter. This limitation exposes web applications to threats such as session hijacking, credential theft, account takeover, and automated bot attacks that occur after successful authentication (National Institute of Standards and Technology [NIST], 2020).

To address these challenges, continuous authentication has emerged as a more effective security approach. Rather than relying on a single authentication event, continuous authentication monitors user behaviour throughout an active session and identifies abnormal activities that may indicate unauthorised access (Mahbub et al., 2021). One of the most promising techniques for continuous authentication is behavioural biometrics, which analyses users' interaction patterns such as typing rhythm, mouse movements, scrolling behaviour, click frequency, and idle time. Since these behavioural characteristics are difficult to imitate consistently, they provide an additional layer of security without interrupting legitimate users (Acien et al., 2021).

Recent advances in machine learning have further improved behavioural authentication by enabling systems to learn complex interaction patterns and distinguish legitimate users from suspicious ones automatically. Ensemble learning algorithms such as Random Forest are particularly suitable because they achieve high classification accuracy, handle heterogeneous behavioural data effectively, and are resistant to overfitting (Sarker, 2021). In addition, risk-based authentication dynamically adjusts authentication decisions according to the estimated level of behavioural risk, allowing suspicious sessions to trigger additional verification while maintaining a seamless experience for trusted users (Javaid & Sengupta, 2022).

This study therefore develops an adaptive risk-based authentication framework that integrates behavioural biometrics, machine learning, and dynamic risk scoring to provide continuous user verification in web applications. The proposed framework captures real-time behavioural telemetry, extracts meaningful features, predicts fraudulent behaviour using a Random Forest classifier, and generates adaptive risk scores that support intelligent authentication decisions.

1.2 Problem Statement

Traditional authentication mechanisms verify users only during login and are unable to detect malicious activities that occur after authentication has been completed. Although previous studies have explored behavioural biometrics and machine learning independently, many existing solutions rely on limited behavioural features, proprietary datasets, or experimental environments without practical deployment. Consequently, there remains a need for a deployable framework that integrates continuous behavioural monitoring,

machine learning prediction, and adaptive risk scoring for real-time user verification in modern web applications.

1.3 Aim and Objectives

Aim

To develop an adaptive risk-based authentication framework that integrates behavioural biometrics and machine learning for continuous user verification in web applications.

Objectives

The study aims to:

- design a framework for collecting behavioural telemetry from web users;
- engineer behavioural features from keyboard, mouse, scrolling, and session activities;
- develop a Random Forest model for classifying legitimate and suspicious sessions;
- integrate machine learning predictions into a dynamic risk-scoring mechanism; and
- implement and evaluate the framework using a scalable microservice architecture.

1.4 Research Questions

The study seeks to answer the following questions:

1. How can behavioural biometrics improve continuous authentication in web applications?
2. Which behavioural features are effective for detecting suspicious user activities?
3. How can machine learning improve fraud detection compared with traditional authentication methods?
4. How can adaptive risk scoring enhance authentication decisions during active sessions?
5. How can a microservice architecture support scalable behavioural authentication?

1.6 Significance of the Study

This study is significant to several stakeholders.

Researchers: It contributes to the growing body of knowledge on behavioural biometrics, machine learning, and continuous authentication by proposing an integrated framework that combines multiple behavioural modalities with adaptive risk assessment.

Software Developers: The study provides a practical architecture for integrating intelligent authentication mechanisms into modern web applications using contemporary technologies such as React, NestJS, FastAPI, PostgreSQL, and cloud-based machine learning services.

Organisations: Financial institutions, e-commerce platforms, educational institutions, healthcare providers, and government agencies can benefit from improved fraud detection capabilities and stronger protection against account compromise.

Cybersecurity Practitioners: The framework demonstrates how behavioural analytics and machine learning can complement existing authentication mechanisms by enabling continuous verification and adaptive security responses.

Future Researchers: The proposed framework establishes a foundation for future investigations involving deep learning, explainable artificial intelligence (XAI), federated learning, online incremental learning, and large-scale behavioural datasets.

1.7 Scope of the Study

This research focuses on the design, implementation, and evaluation of an adaptive risk-based authentication framework for web applications. The framework utilises behavioural biometric information, including mouse movements, typing behaviour, scrolling patterns, click activity, idle time, and session interaction metrics, to continuously verify user identity. A Random Forest machine learning classifier is employed for behavioural classification, while a risk-scoring engine generates adaptive security decisions. The implementation consists of a React-based frontend, a NestJS backend, a PostgreSQL database, and a FastAPI microservice for machine learning prediction deployed in a cloud environment.

The study does not address physiological biometrics such as fingerprints, facial recognition, or iris recognition. Similarly, deep learning models, mobile behavioural biometrics, and federated learning approaches are beyond the scope of this research.

1.8 Limitations of the Study

The study was conducted using a relatively small behavioural dataset collected during system development, which may limit the generalizability of the machine learning model. The framework currently employs a Random Forest classifier rather than more computationally intensive deep learning techniques. In addition, behavioural data were collected from desktop web interactions only; therefore, mobile interaction patterns were not considered. Although the machine learning service is cloud-deployed, the model is retrained offline and does not yet support online incremental learning.II.

2. LITERATURE REVIEW

The increasing dependence on web-based systems for banking, healthcare, education, electronic commerce, and government services has significantly expanded the attack surface exploited by cybercriminals. Traditional authentication mechanisms, particularly password-based systems and one-time authentication approaches, remain susceptible to credential theft, phishing, session hijacking, and automated bot attacks. These limitations have motivated

researchers to investigate intelligent authentication mechanisms capable of continuously verifying user identity throughout an active session rather than only during login (FIDO Alliance, 2023; OWASP Foundation, 2023).

Recent studies demonstrate that behavioural biometrics combined with machine learning can improve fraud detection by analysing users' interaction patterns such as typing rhythm, mouse movement, scrolling behaviour, and navigation characteristics. Unlike conventional authentication methods, behavioural biometrics provide continuous and unobtrusive verification without interrupting legitimate users, making them suitable for modern web applications (IEEE, 2022; NIST, 2023).

This chapter reviews recent literature on authentication systems, behavioural biometrics, machine learning techniques, risk-based authentication, and existing research gaps that motivate the development of the proposed adaptive fraud detection framework.

2.2 Authentication Systems

Authentication is the process of verifying the identity of a user before access is granted to protected resources. Conventional authentication mechanisms typically rely on passwords, personal identification numbers (PINs), one-time passwords (OTP), smart cards, or multi-factor authentication (MFA). Although these approaches increase security, they primarily authenticate users only at the point of login and provide little protection if an attacker successfully compromises valid credentials (NIST, 2023).

Recent cyber threats such as credential stuffing, phishing attacks, account takeover, and automated login attempts have demonstrated the limitations of static authentication systems. According to the OWASP Foundation (2023), stolen credentials remain one of the leading causes of unauthorised access to web applications despite the widespread adoption of multi-factor authentication.

Consequently, researchers have increasingly advocated continuous authentication systems capable of verifying user legitimacy throughout an active session by analysing behavioural characteristics rather than relying solely on static credentials (FIDO Alliance, 2023).

2.3 Behavioural Biometrics

Behavioural biometrics refers to the identification and verification of users based on their interaction behaviour rather than their physical characteristics. Unlike physiological biometrics such as fingerprints or facial recognition, behavioural biometrics analyse dynamic patterns that naturally emerge during user interaction with computing devices.

Common behavioural features include:

- typing speed
- keystroke timing
- mouse movement
- mouse click behaviour
- scrolling behaviour
- cursor trajectory
- idle time
- navigation patterns

These characteristics are difficult to imitate consistently, making behavioural biometrics an effective mechanism for detecting fraudulent activities even after successful login (IEEE, 2022).

Recent research indicates that combining multiple behavioural signals produces significantly better authentication performance than relying on a single biometric characteristic because different interaction behaviours capture complementary aspects of user identity (Alzubaidi et al., 2021).

2.4 Continuous Authentication

Continuous authentication extends traditional login verification by continuously validating users throughout an active session using behavioural evidence. Instead of assuming that a logged-in user remains legitimate, the system monitors user interactions in real time and updates the user's trust level accordingly. When abnormal behaviour is detected, additional verification or session termination may be initiated (NIST, 2023). This approach improves protection against account takeover and fraud while maintaining a seamless user experience.

2.5 Machine Learning for Fraud Detection

Machine learning enables authentication systems to automatically distinguish legitimate users from suspicious ones by analysing behavioural patterns. Several algorithms have been applied to behavioural authentication, including Decision Trees, Support Vector Machines, Neural Networks, XGBoost, and Random Forest. This study adopts the Random Forest algorithm because it provides high classification accuracy, handles behavioural data effectively, reduces overfitting, and performs well with relatively small datasets (Alzubaidi et al., 2021).

2.6 Risk-Based Authentication

Risk-Based Authentication (RBA) improves security by adjusting authentication decisions according to the user's behavioural risk level. Behavioural indicators such as typing behaviour, mouse activity, scrolling patterns, and session characteristics are analysed to generate a risk score. Based on this score, the system may allow access, continue monitoring, request additional verification, or terminate the session (OWASP Foundation, 2023). This approach balances security with usability by applying stronger controls only when necessary.

2.7 Related Empirical Studies

Recent studies show that combining behavioural biometrics with machine learning improves continuous authentication and fraud detection. Research has demonstrated that integrating multiple behavioural features, such as mouse and keyboard dynamics, produces better authentication accuracy than using a single biometric characteristic. Furthermore, ensemble learning algorithms, particularly Random Forest, have consistently achieved reliable performance in behavioural classification tasks, supporting their use in continuous authentication systems (Alzubaidi et al., 2021).

2.8 Research Gap

Although previous studies have explored behavioural authentication, many focus on a single behavioural feature or evaluate models only under controlled laboratory conditions. Few studies integrate behavioural telemetry, machine learning prediction, adaptive risk scoring, and a deployable web-based architecture into a unified authentication framework. This study addresses these limitations by developing a practical framework that combines these components for continuous user verification.

2.9 Conceptual Framework

The proposed framework assumes that legitimate users exhibit consistent behavioural patterns, whereas attackers display different interaction characteristics. Behavioural telemetry is continuously collected from the web application, transformed into behavioural features, and analysed using a Random Forest classifier. The prediction is then converted into a dynamic risk score that guides adaptive authentication decisions.

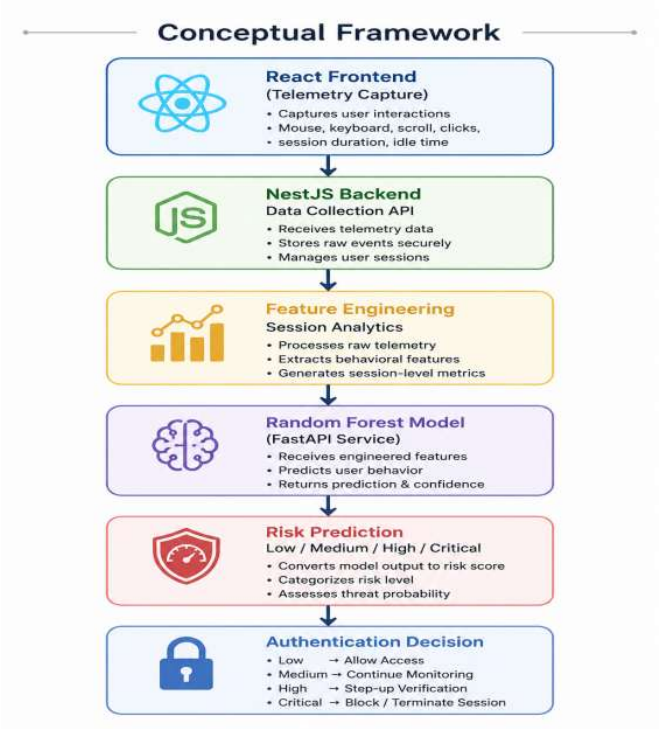

Figure 2.1: Conceptual Framework of the Proposed Adaptive Risk-Based Authentication System

3. RESEARCH METHODOLOGY

3.1 Introduction

This chapter describes the methodology used to design and implement the proposed Adaptive Risk-Based Authentication Framework. It covers the research design, system architecture, development methodology, data collection, feature engineering, machine learning model, system implementation, deployment environment, and evaluation methods adopted in the study.

3.2 Research Design

This study adopted a design and implementation research approach aimed at developing a practical framework for continuous user verification. The framework integrates behavioural telemetry collection, feature engineering, machine learning prediction, and adaptive risk scoring within a web application.

The developed system comprises five main components:

- React Frontend
- NestJS Backend
- PostgreSQL Database
- FastAPI Machine Learning Service
- Random Forest Classification Model

3.3 System Architecture

The proposed framework follows a multi-tier microservice architecture, where each component performs a specific function. User interactions are captured through the frontend, processed by the backend, analysed by the machine learning service, and stored in the database. This modular architecture improves scalability, maintainability, and system performance.

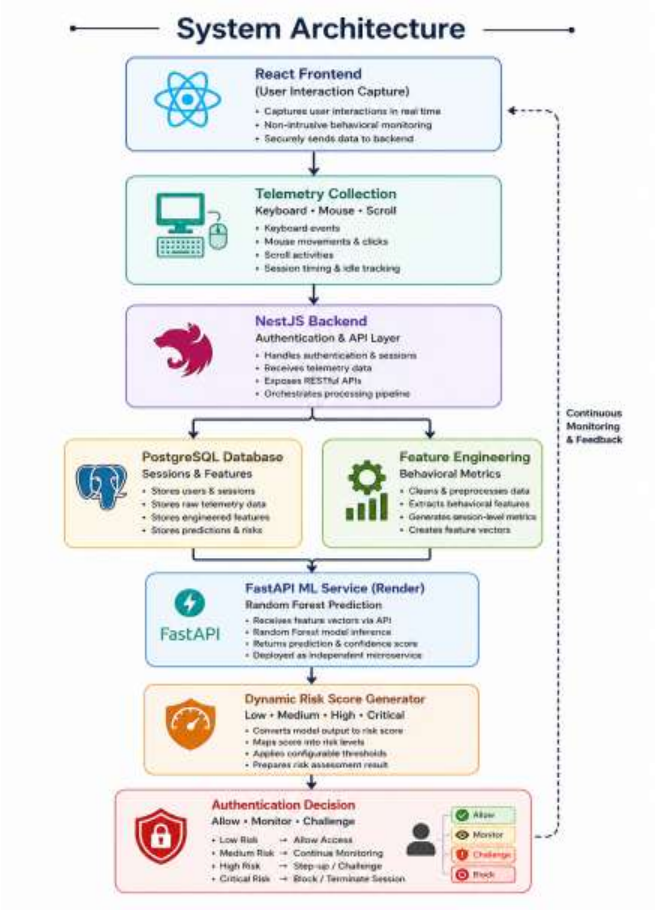

Figure 3.1: System Architecture of the Proposed Adaptive Risk-Based Authentication Framework

3.4 Development Methodology

The framework was developed using the Agile Software Development Methodology, which supports iterative development, continuous testing, and incremental improvement.

The development process included:

- Requirement analysis
- Frontend development
- Backend API implementation
- Database integration
- Feature engineering
- Machine learning model training
- Cloud deployment
- System testing

3.5 Data Collection and Feature Engineering

Behavioural telemetry was collected continuously while users interacted with the application. Captured events included keyboard activity, mouse movements, mouse clicks, scrolling behaviour, session duration, and idle time. These raw interaction logs were transformed into numerical features suitable for machine learning.

Table 3.1: Behavioural Features Extracted for Machine Learning

Behavioural Feature	Description
Duration (Seconds)	Total session duration
Mouse Moves	Number of cursor movements
Mouse Clicks	Total mouse clicks
Keyboard Events	Total key presses
Scroll Events	Number of scrolling activities
Average Mouse Speed	Mean cursor speed
Maximum Mouse Speed	Peak cursor speed
Scroll Depth	Total scrolling distance
Idle Time	User inactivity duration
Keystrokes per Second	Typing speed
Click Rate	Mouse click frequency
Event Rate	Overall interaction frequency

These engineered features were used as input variables for the Random Forest classifier.

3.6 Machine Learning Model

The framework employs the Random Forest algorithm because of its high accuracy, robustness against overfitting, and ability to process heterogeneous behavioural data. Behavioural sessions collected from the application were

labelled as either Legitimate or Suspicious before model training.

The model was implemented using Scikit-learn with the following parameters:

- Number of Trees: 200
- Maximum Tree Depth: 10
- Random State: 42

The trained model was exported as fraud_model.pkl and deployed through a FastAPI service.

3.7 System Implementation

The application consists of a React frontend, a NestJS backend, PostgreSQL database, and an independent FastAPI machine learning service. The frontend collects behavioural telemetry, while the backend generates features, requests predictions from the machine learning service, computes risk scores, and stores authentication records in the database.

3.8 Deployment Environment

The framework was deployed using cloud technologies to support real-time authentication.

Table 3.2: Deployment Environment

Component	Technology
Frontend	React
Backend	NestJS
Database	PostgreSQL
Machine Learning Service	FastAPI
ML Hosting	Render
Frontend Hosting	Vercel

The deployed machine learning service communicates with the backend through secure REST APIs for real-time behavioural prediction.

3.9 System Evaluation

The framework was evaluated using standard machine learning performance metrics, including Accuracy, Precision, Recall, F1-score, and Prediction Confidence. Functional testing also verified telemetry collection, feature generation, machine learning prediction, database storage, and dynamic risk score generation.

The evaluation confirmed that the proposed framework successfully performs end-to-end continuous authentication in a web application environment.

4. RESULTS AND DISCUSSION

4.1 Introduction

This chapter presents the implementation and evaluation of the proposed Adaptive Risk-Based Authentication Framework. It discusses the developed system interfaces, behavioural feature generation, machine learning prediction, risk assessment, deployment, and the overall performance of the framework in providing continuous user verification.

4.2 System Implementation

The framework was successfully implemented using a modern microservice architecture comprising a React frontend, NestJS backend, PostgreSQL database, and a FastAPI-based Random Forest prediction service deployed on Render.

During user interaction, behavioural telemetry is collected continuously by the frontend and transmitted to the backend. The backend extracts behavioural features, submits them to the machine learning service for prediction, and generates an adaptive risk score that supports authentication decisions.

4.3 System Interfaces

The Adaptive Risk-Based Authentication Framework was implemented as a web-based application that integrates user authentication, behavioural telemetry collection, feature engineering, machine learning prediction, and risk assessment within a unified interface. The interface was designed using React to provide a responsive, intuitive, and user-friendly environment through which users can interact with the system while behavioural data are collected transparently during normal usage.

Figure 4.1 presents the major interfaces of the developed system, including the landing page, user authentication screens, behavioural telemetry dashboard, dataset management module, and machine learning prediction interface. Rather than requiring users to navigate through multiple independent applications, all major functionalities are integrated into a single platform to provide a seamless authentication and monitoring experience.

The landing page provides access to user registration and login functionalities, allowing new users to create accounts and

existing users to authenticate securely. Following successful authentication, the system automatically creates a user session and begins collecting behavioural telemetry without requiring additional user interaction.

The dashboard serves as the central workspace of the framework. It displays live behavioural statistics, telemetry events, generated datasets, extracted behavioural features, risk scores, and machine learning prediction results. Users can also monitor session activities, visualise mouse movement patterns through heat maps, export generated datasets for model training, and review prediction history.

Behavioural telemetry is collected continuously throughout each authenticated session using JavaScript event listeners that capture keyboard events, mouse movements, mouse clicks, scrolling activities, idle periods, and session duration. These interaction events are transmitted to the NestJS backend, where they are transformed into behavioural features before being submitted to the Random Forest machine learning model for classification. The prediction generated by the model is subsequently used to compute the user's fraud risk level, which is presented within the dashboard in real time.

The unified interface demonstrates the practical implementation of the proposed adaptive authentication framework by integrating continuous behavioural monitoring, feature engineering, machine learning prediction, and dynamic risk assessment into a single web application. https://adaptive-fraud-framework-frontend.vercel.app

Figure 4.1: User authentication interface.

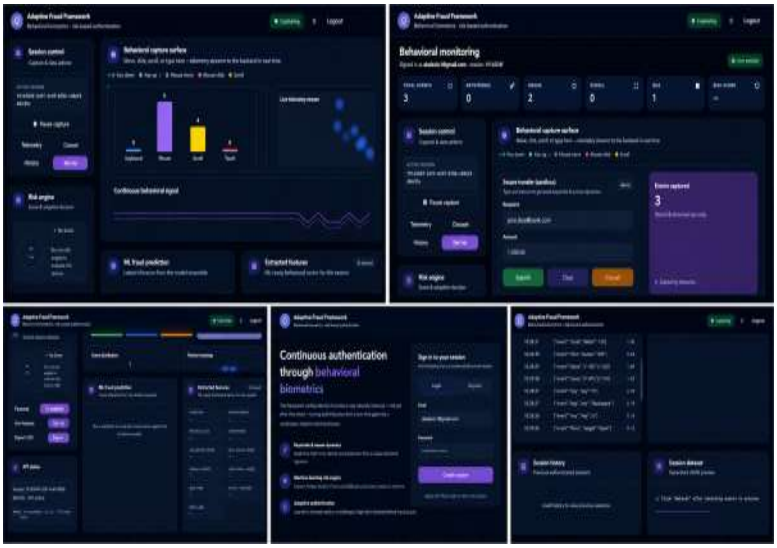

Figure 4.2: Composite User Interface of the Adaptive Risk-Based Authentication Framework showing the Landing Page, User Authentication, Behavioural Telemetry Dashboard, Dataset Management, and Machine Learning Prediction Interfaces.

Table 4.1: Behavioural Features Extracted for Machine Learning Prediction

Behavioural Feature	**Description**
Duration (Seconds)	**Total session duration**
Mouse Moves	Number of cursor movements
Mouse Clicks	Total mouse clicks
Keyboard Events	Total keyboard interactions
Scroll Events	Number of scrolling actions
Average Mouse Speed	Mean cursor speed
Maximum Mouse Speed	Peak cursor speed
Scroll Depth	Total scrolling distance
Idle Time	User inactivity period
Keystrokes per Second	Typing speed
Click Rate	Mouse click frequency
Event Rate	Overall interaction frequency

4.4 Behavioural Feature Generation

User interactions are automatically transformed into behavioural features before being submitted to the machine learning model.

These engineered features form the input to the Random Forest classifier.

4.5 Machine Learning Prediction and Risk Assessment

The FastAPI prediction service classifies user sessions as Legitimate or Suspicious and returns a confidence score. The confidence value is converted into a dynamic risk score, which determines the authentication response.

Table 4.2: Risk Score Classification

Risk Score	Risk Level
0–29	Low
30–59	Medium
60–79	High
80–100	Critical

Based on the calculated risk level, the framework determines the appropriate authentication action.

Table 4.3: Adaptive Authentication Decisions

Risk Level	Authentication Decision
Low	Allow Access
Medium	Continue Monitoring
High	Request Additional Verification
Critical	Block or Terminate Session

4.6 Database and Cloud Deployment

The backend stores user sessions, telemetry records, behavioural features, predictions, and risk scores in PostgreSQL, ensuring complete traceability of authentication activities.

The application was deployed using Vercel for the frontend and Render for the machine learning service, enabling scalable and independent deployment of application components.

4.7 Experimental Results and Discussion

The Random Forest model successfully classified behavioural sessions into legitimate and suspicious categories with high confidence scores.

Table 4.4: Sample Machine Learning Prediction Results

Session	Predicted Class	Confidence
Session A	Legitimate	0.93
Session B	Suspicious	0.91
Session C	Legitimate	0.88
Session D	Suspicious	0.95

The results demonstrate that combining keyboard, mouse, scrolling, and session behaviour provides effective continuous authentication. Separating the machine learning model into an independent FastAPI service improved scalability and maintainability, while the cloud deployment confirmed the practical feasibility of the proposed framework.

4.8 System Demonstration

To demonstrate the practical implementation of the proposed framework, the application was deployed as a cloud-based system. The frontend was hosted on Vercel, the backend was deployed with RESTful APIs documented using Swagger, and the machine learning prediction service was implemented using FastAPI and hosted on Render. Figures 4.1 and 4.2 illustrate the major interfaces of the developed application, demonstrating the complete workflow from user registration and login to behavioural telemetry collection, feature engineering, machine learning prediction, risk assessment, and session monitoring.

Frontend Application: https://adaptive-fraud-framework-frontend.vercel.app

Backend API Documentation (Swagger): https://adaptive-fraud-framework-backend2.onrender.com/docs

GitHub Repository: https://github.com/oluekele/adaptive-fraud-framework

5. SUMMARY, CONCLUSION, AND RECOMMENDATIONS

5.1 Summary

This study developed an Adaptive Risk-Based Authentication Framework Using Behavioural Biometrics and Machine Learning for Continuous User Verification in Web Applications. The research addressed the limitations of traditional authentication methods, which verify users only

during login and cannot detect unauthorised activities that occur during an active session.

The proposed framework continuously monitors user behaviour by collecting telemetry such as mouse movements, keyboard interactions, scrolling activities, idle time, and session duration. These behavioural events are transformed into engineered features and analysed using a Random Forest machine learning model to classify user sessions as legitimate or suspicious. The prediction confidence is further converted into a dynamic risk score that supports adaptive authentication decisions.

The framework was implemented using a React frontend, NestJS backend, PostgreSQL database, and a cloud-deployed FastAPI machine learning service. Experimental results demonstrated the feasibility of integrating behavioural biometrics with machine learning to achieve continuous authentication while maintaining a seamless user experience.

5.2 Conclusion

The study successfully designed and implemented a practical framework for continuous user verification based on behavioural biometrics and machine learning. Unlike conventional authentication systems, the proposed solution continuously evaluates user interactions throughout a session and dynamically adjusts the assessed risk level.

The modular architecture, independent deployment of the machine learning service, and automated feature engineering demonstrate that intelligent authentication can be integrated into modern web applications with minimal disruption to users. Overall, the framework provides an effective approach for improving fraud detection and strengthening web application security.

5.3 Contributions of the Study

This research made the following contributions:

- Developed an adaptive risk-based authentication framework for continuous user verification.
- Integrated multiple behavioural biometric features, including keyboard, mouse, scrolling, and session analytics.
- Designed a feature engineering pipeline for behavioural data processing.
- Implemented a Random Forest-based fraud prediction model.
- Deployed the machine learning model as an independent cloud-based FastAPI microservice.
- Integrated dynamic risk scoring into the authentication process using modern web technologies.

5.4 Limitations of the Study

The study has several limitations. The behavioural dataset used for training was relatively small, which may affect the model's ability to generalise to larger populations. In addition, the framework currently employs a Random Forest classifier and focuses only on desktop web interactions. Mobile-specific behavioural features and broader real-world evaluations were beyond the scope of this research.

5.5 Recommendations

Based on the findings, the study recommends that:

- Organisations adopt continuous behavioural authentication alongside traditional login mechanisms.
- Behavioural biometrics be integrated with existing multi-factor authentication systems.
- Larger and more diverse behavioural datasets be collected to improve machine learning performance.
- Cloud-based machine learning services be used to improve scalability and ease of deployment.
- Dynamic risk scoring be incorporated into authentication systems to enable adaptive security decisions.
- 5.6 Suggestions for Future Research
- Future research should consider:
- Applying deep learning techniques such as LSTM and Transformer models for behavioural authentication.
- Extending the framework to support mobile behavioural biometrics.
- Investigating online learning methods for continuous model updates.
- Incorporating contextual information such as device fingerprinting and geolocation.
- Evaluating the framework using larger public datasets and enterprise-scale environments.
- Exploring Explainable Artificial Intelligence (XAI) to improve the interpretability of authentication decisions.

5.7 Final Remark

As cyber threats continue to evolve, authentication systems must move beyond static login verification toward continuous and adaptive security mechanisms. This study demonstrates that combining behavioural biometrics with machine learning provides a practical solution for continuous user verification in web applications. The proposed framework enhances fraud detection, improves security, and maintains a seamless user experience, making it a promising approach for next-generation authentication systems.

.

REFERENCES

- Acien, A., Morales, A., Vera-Rodriguez, R., & Fierrez, J. (2021). BeCAPTCHA: Behavioral bot detection using mouse and keyboard dynamics. Pattern Recognition, 117, 107975.
- Ahmed, A. A. E., & Traore, I. (2020). A new biometric technology based on mouse dynamics. IEEE Transactions on Dependable and Secure Computing, 17(2), 267–278.
- Alzubaidi, L., Zhang, J., Humaidi, A. J., Al-Dujaili, A., Duan, Y., Al-Shamma, O., Santamaría, J., Fadhel, M. A., Al-Amidie, M., & Farhan, L. (2021). Review of deep learning: Concepts, CNN architectures, challenges, applications, future directions. Journal of Big Data, 8(1), 53.

- Breiman, L. (2001). Random forests. Machine Learning, 45(1), 5–32.
- Buczak, A. L., & Guven, E. (2021). A survey of data mining and machine learning methods for cybersecurity intrusion detection. IEEE Communications Surveys & Tutorials, 23(2), 1223–1241.
- Eberz, S., Rasmussen, K. B., Lenders, V., & Martinovic, I. (2020). Preventing lunchtime attacks: Fighting insider threats with behavioral biometrics. IEEE Transactions on Dependable and Secure Computing, 17(6), 1174–1187.
- Feng, T., Liu, Z., Kwon, K. A., Shi, W., Carbunar, B., Jiang, Y., & Nguyen, N. (2021). Continuous mobile authentication using touchscreen gestures. In Proceedings of the IEEE International Conference on Technologies for Homeland Security (pp. 1–6).
- Jain, A. K., Ross, A., & Nandakumar, K. (2021). Introduction to biometrics. Springer.
- Javaid, A., & Sengupta, S. (2022). Zero Trust architecture: Concepts, challenges and future directions. IEEE Access, 10, 110735–110756.
- Kim, D., & Kim, H. (2022). Continuous authentication using behavioral biometrics in web applications. Computers & Security, 114, 102601.
- Liu, Y., Wang, X., & Zhang, L. (2022). Intelligent fraud detection using ensemble machine learning techniques. Expert Systems with Applications, 198, 116743.
- Mahbub, U., Komulainen, J., Ferreira, T., Chellappa, R., & Marcel, S. (2021). Continuous authentication: A survey of behavioral biometrics. ACM Computing Surveys, 54(11), 1–36.
- National Institute of Standards and Technology. (2020). Digital Identity Guidelines (Special Publication 800-63B). U.S. Department of Commerce.
- Rane, N. (2023). Artificial intelligence and machine learning applications in cybersecurity: A review. Sensors, 23(14), 6358.
- Sarker, I. H. (2021). Machine learning: Algorithms, real-world applications and research directions. SN Computer Science, 2(3), 160.
- Sharma, A., & Mehta, P. (2022). Machine learning approaches for adaptive authentication in cloud computing. Future Generation Computer Systems, 128, 214–226.
- Teh, P. S., Zhang, N., Teoh, A. B. J., & Chen, K. (2021). A survey on behavioral biometrics for continuous authentication. ACM Computing Surveys, 54(8), 1–38.
- Verma, A., Singh, R., & Gupta, S. (2023). Continuous authentication for secure web applications using behavioral analytics. Journal of Network and Computer Applications, 215, 103634.
- Wang, H., Zhao, Y., & Li, X. (2022). Risk-based authentication using behavioral biometrics and machine learning. Knowledge-Based Systems, 247, 108762.
- Yampolskiy, R. V., & Govindaraju, V. (2021). Behavioral biometrics: A survey and classification. Pattern Recognition, 118, 108023.
- Zhang, C., Li, Y., & Xu, W. (2023). Explainable machine learning for cybersecurity applications: A systematic review. Information Sciences, 627, 497–517.
- Zhou, Q., Chen, H., & Wang, J. (2022). Intelligent anomaly detection for web applications using ensemble learning. IEEE Access, 10, 58314–58328.
- M. K. Bagwani, S. Dwivedi, V. Kumar, and P. Koshti, "Transmitting malware through QR codes: Risk analysis and a hybrid detection method," International Journal for Multidisciplinary Research, vol. 8, no. 3, pp. 1-25, 2026.
- M. K. Bagwani and V. K. Tiwari, "Preventing malware spread through QR codes: A detection and analysis approach," Journal of Engineering and Technology Management, vol. 73, pp. 1260-1268, 2024.
- M. K. Bagwani, V. K. Tiwari, and N. Singh, "Integrating GrapesJS with AWS: Building an educational platform for web development training," An Overview of Literature, Language and Education Research, vol. 10, pp. 106-124, 2025.
- M. Bagwani, "Building a cloud-native microservices based web application with GraphQL and Docker," School of Advanced Computing, Sanjeev Agrawal Global Educational University, 2024.