Continuous Adaptive Trust Framework for Enhancing Authentication Using Real-Time User Behaviour Analytics

Tharaka Wijekoon

229408C

Master of Science in Computer Science

Department of Computer Science & Engineering
Faculty of Engineering

University of Moratuwa
Sri Lanka

June 2025

Continuous Adaptive Trust Framework for Enhancing Authentication Using Real-Time User Behaviour Analytics

Tharaka Wijekoon

229408C

Thesis/Dissertation submitted in partial fulfillment of the requirements for the degree Master of Science in Computer Science

Department of Computer Science & Engineering
Faculty of Engineering

University of Moratuwa
Sri Lanka

June 2025

DECLARATION

I declare that this is my own work and this thesis/dissertation does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any other University or Institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text. I retain the right to use this content in whole or part in future works (such as articles or books).

Signature: Tharaka Wijekoon Date: 01/06/2025

The above candidate has carried out research for the PhD/MPhil/Masters thesis/dissertation under my supervision. I confirm that the declaration made above by the student is true and correct.

Name of Supervisor: Prof. Indika Perera

Signature of the Supervisor: Date:

ABSTRACT

Traditional authentication systems struggle to address the dynamic nature of modern cyber threats, often relying on static rules or historical data that fail to adapt to real-time risks. This research proposes a Framework for Continuous Adaptive Trust (CAT) designed to enhance adaptive authentication by integrating real-time user behavior analytics. The framework dynamically assesses contextual factors—including login time, geolocation, device type, and access patterns—to construct behavioral baselines, detect anomalies through hybrid statistical and machine learning models, and enforce adaptive authentication policies. By leveraging a weighted trust score $Ttotal$ that combines behavioral analytics with multi-factor authentication (MFA) outcomes, the system aims to balance security and usability. Integration with the WSO2 Identity Server demonstrates feasibility for enterprise Identity and Access Management (IAM) systems. This work addresses critical gaps in adaptive authentication by prioritizing real-time adaptability, scalability, and privacy-conscious design, offering a foundation for resilient cybersecurity solutions in evolving threat landscapes.

Keywords: Adaptive authentication, user behavior analytics, continuous trust, risk-based authentication, cybersecurity

Table of Contents

List of Figures

List of Tables

List of Abbreviations

Abbreviation	Description
ACM	Association for Computing Machinery
AI	Artificial Intelligence
CAT	Continuous Adaptive Trust
GDPR	General Data Protection Regulation
IAM	Identity and Access Management
IEEE	Institute of Electrical and Electronic Engineers
IoT	Internet of Things
MFA	Multi-Factor Authentication
ML	Machine Learning
OTP	One-Time Password
RBA	Risk-Based Authentication
UBA	User Behavior Analytics
DL	Deep learning
TPR	True Positive Rate
FPR	False Positive Rate
TNR	True Negative Rate
FNR	False Negative Rate
AUC	Area Under ROC Curve
LSTM	Long Short-Term Memory
CCPA	California Consumer Privacy Act
RAT	Remote Access Trojans
SIEM	Security Information and Event Management