

LB/TH/43/2025  
TH6014

# **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  $T_{total}$  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

Declaration.....	i
Abstract.....	ii
Table of Contents.....	iii
List of Figures.....	v
List of Tables.....	vi
List of Abbreviations.....	vii
1 Introduction.....	1
1.1 Background.....	1
1.2 Research Problem.....	4
1.3 Research Objectives.....	4
1.4 Thesis Structure.....	4
2 Literature Review.....	6
2.1 Background.....	6
2.2 Previous Studies and Findings.....	8
2.2.1 Current Techniques in Adaptive Authentication.....	9
2.2.2 Challenges and Limitations.....	12
2.2.3 Future Directions.....	14
3 Proposed method.....	18
3.1 Authentication Data Collection.....	18
3.2 Behavioral Analysis and Anomaly Detection.....	20
3.2.1 Statistical Anomaly Z-Score.....	21
3.2.2 Deep learning Model.....	23
3.2.3 Composite Hybrid Anomaly Score.....	24
3.3 Dynamic Risk Assessment.....	25
3.4 System Integration.....	25
3.5 Testing and Evaluation.....	26
4 Implementation.....	27
4.1 System Architecture Overview.....	27
4.2 Data Collection Module.....	27
4.2.1 Implementation Overview.....	28
4.2.2 Key Components of the UBATracker Script.....	28
4.2.3 Integration with WSO2 Identity Server.....	31
4.3 Behavioral Baseline Modeling.....	31
4.3.1 Baseline Establishment Workflow.....	31
4.3.2 Sliding Window Baseline.....	32
4.4 Data Processing.....	33
4.4.1 Z-Score Standardization.....	33

4.4.2	How each feature is standardized.....	33
4.5	Hybrid Anomaly Detection Model.....	34
4.5.1	Statistical Z-Score Model.....	34
4.5.1.1	Multi-dimensional Behavioral Analysis.....	35
4.5.1.2	Euclidean Norm Score Aggregation.....	35
4.5.2	Deep Learning Model.....	35
4.5.2.1	Sequential Data Processing.....	36
4.5.2.2	Static Feature Integration.....	36
4.5.2.3	Network Architecture and Training.....	37
4.5.2.4	User-Specific Model Training.....	37
4.5.2.5	Model Persistence and Efficiency.....	38
4.6	Dynamic Policy Enforcement.....	38
4.6.1	Policy Enforcement Workflow.....	38
4.6.2	Authentication Script Structure.....	40
4.6.3	Trust Score Calculation.....	40
4.6.4	Conditional MFA Enforcement.....	40
4.7	Performance Optimization.....	42
4.7.1	In-Memory Model Caching.....	42
4.7.2	Optimized Database Schema.....	42
5.	Results and Discussion.....	44
5.1	Model Performance Evaluation.....	44
5.1.1	Experimental Setup.....	44
5.1.2	Statistical Model Performance.....	46
5.1.3	Deep Learning Model Performance.....	49
5.1.4	Hybrid Model Performance.....	53
5.1.5	Cold Start Performance Analysis.....	55
5.2	User Experience Impact.....	57
5.2.1	Authentication Friction Reduction.....	58
5.2.2	User Satisfaction Metrics.....	60
5.3	Latency Benchmarks.....	62
5.4	Limitations.....	63
5.5	Future Work.....	65
6	Conclusion.....	67
	References.....	69

## LIST OF FIGURES

<b>Figure</b>	<b>Description</b>	<b>Page</b>
Figure 1	Authentication Factors	6
Figure 2	Proposed Framework Architecture	19
Figure 3	Workflow of trust score calculation	21
Figure 4	Benefit of using DL over traditional ML methods.	24
Figure 5	Components of the trust score $T_{total}(t)$	26
Figure 6	Implemented System Architecture	28
Figure 7	Data flow client to server	29
Figure 8	Serialized data embedded in login request	32
Figure 9	New tables for the behavior baseline tracking	33
Figure 10	New table created to storing the DL model data	39
Figure 11	Conditional logic for MFA enforcement	40
Figure 12	Example flow with 2 MFA steps and default settings	42
Figure 13	Statistical Model Accuracy vs. Window Size	49
Figure 14	Relative contribution of each behavioral dimension.	50
Figure 15	DL Model Performance vs. Training Iterations	52
Figure 16	Detection Rate vs. Imitation Attack Sophistication	53
Figure 17	ROC Curves for Model Comparison	55
Figure 18	Model Accuracy vs. Available Training Sessions	57
Figure 19	MFA Prompt Reduction by Risk Level	59
Figure 20	User Satisfaction Scores Pre and Post Implementation	61
Figure 21	Load test results for before and after implementation	63

## LIST OF TABLES

<b>Table</b>	<b>Description</b>	<b>Page</b>
Table 1	Comparison of Adaptive Authentication Techniques	12
Table 2	Data Collection Parameters	20
Table 3	Planned Evaluation Metrics	27
Table 4	Device Information Parameters	31
Table 5	Feature standardization	34
Table 6	Baseline statistics for hypothetical user	35
Table 7	Performance Metrics for Statistical Z-Score Model	48
Table 8	Performance Metrics for Deep Learning Model	51
Table 9	Performance Metrics for Hybrid Adaptive Model	54
Table 10	MFA Prompt Frequency Analysis	60

## LIST OF ABBREVIATIONS

<b>Abbreviation</b>	<b>Description</b>
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