

**USER INTERACTIVE AND SMART ADAPTIVE
AUTHENTICATION FOR WEB-BASED
APPLICATIONS**

Mohamed Riyazath Ali

209304K

Degree of Master of Science

Department of Computer Science and Engineering

University of Moratuwa
Sri Lanka

2020

**USER INTERACTIVE AND SMART ADAPTIVE
AUTHENTICATION FOR WEB-BASED
APPLICATIONS**

Mohamed Riyazath Ali

209304K

Degree of Master of Science

Department of Computer Science and Engineering

University of Moratuwa
Sri Lanka

2020

The declaration of the author

I declare that this is my own work, and this dissertation does not incorporate without acknowledgement any material previously submitted for 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.

Also, I hereby grant to the University of Moratuwa the non-exclusive right to reproduce and distribute my dissertation, in whole or in part in print, electronic or other media. I retain the right to use this content in whole or part in future works (such as articles or books).

Signature:

Date:

Name: I.L.M. Riyazath Ali.

The supervisor/s should certify the thesis/dissertation with the following declaration.

I certify that the declaration above by the candidate is true to the best of my knowledge and that the above candidate has carried out research for the Masters Dissertation(CS6997 MSc Research Project) under my supervision.

Signature of the supervisor:

Date:

Name: Dr. Indika Perera

Head - Dept. of Computer Science & Engineering, Faculty of Engineering

University of Moratuwa, Moratuwa 10400, Sri Lanka.

The abstract

Authentication is a way to verify identification of users. Authentication plays a crucial part in safeguarding the data. Currently, nearly any form of data is saved on the Internet, which makes security concerns of the private data extremely vital. Initially, single factor authentication was employed to safeguard data and identify identity. Because of the rising security vulnerabilities in single factor authentication, two/multi factor authentication was created. The multi-factor authentication has an unfavorable influence on user experience. The additional authentication layer impacts the user friendliness/user experience of a given application, and the user must spend more time in the extra authentication step to confirm the identity. Adaptive authentication was built to overcome this problem. Adaptive Authentication determines the optimal authentication method for a user dependent on context parameters such as behavioral traits, location, network, and certain other user features. This technology has the capacity of modifying the standard authentication (i.e. username/password) technique and directing it in a more secure and user-friendly direction. Existing work will be analyzed in this research, and a better adaptive authentication mechanism will be created and deployed. Adaptable Auth is a novel adaptive authentication design. This research offers a revolutionary adaptive authentication technique which seeks to erase the bad user experience of the existing multi factor authentication systems. Adaptive authentication accumulates information about each user and prevents fraudulent attempts by checking them against the generated profiles. This technique will boost the usability, user-friendliness by adding multi-factor authentication only when its essential utilizing a risk based adaptive approach. Furthermore, the solution maintains security by authenticating the genuine user via jointly assessing the attributes, behavior, device and network relevant information. Separate machine learning models will be deployed to identify the user based on user behavior and circumstance. This research presents a novel technique to enhancing the overall performance of the authentication process. The authentication mechanisms will be selected depending on the user's risk profile. This enhances the authentication process's user experience.

Key words: Adaptive authentication, Machine learning Mouse and keystroke dynamics

Acknowledgements

I like to communicate sincere thanks and gratefulness to my MSc Research Project supervisor, Dr. Indika Perera, guiding me through all semesters and unconditionally aiding me in acquiring all needed resources to achieve my MSc Research Project Thesis.

I am particularly thankful for his major help in the research effort, which included giving the required skills, resources, guidance, supervision, and beneficial suggestions. With his expertise and constant help, I was able to finish my study properly. I would also like to thank all my colleagues for their aid and support in discovering pertinent study material. I am extremely thankful to my parents, brothers, sister, nephew, niece, and close friends for their support. Finally, I would like to convey my appreciation to all my fellow members for their aid in managing my MSc studies. Moreover, I want to offer thankfulness to the personalities since they have supported me during this effort.

TABLE OF CONTENTS

The declaration of the author	ii
The abstract	iii
Acknowledgements	iv
LIST OF FIGURES	viii
LIST OF TABLES	ix
LIST OF ABBREVIATIONS	x
1. Chapter	1
1. Introduction	1
1.1. Overview of the chapter	1
1.2. Introduction	1
1.3. Background	2
1.4. Related Work	5
1.4.1. Existing work on behaviour based adaptive authentication	6
1.4.2. Existing work on user context based adaptive authentication	8
1.5. Problem in brief	11
1.6. Research Motivation	11
1.7. Aim and Objectives	13
1.7.1 Research Aim	15
1.7.2. Research Objectives	15
1.8. Chapter Synopsis	17
2. Chapter	18
2. Critical Literature Review Survey	18
2.1. Overview of the chapter	18
2.2. Description of the Area of Expertise	18
2.2.1. An Overview of Authentication Mechanism	18
2.2.2 Type of authentication methods based on the category.	19
2.2.3. An Overview of Adaptive Authentication	20
2.2.4. Adaptive Authentication System Architecture	24
2.3. Technological Review	25
2.3.1 User attribute based adaptive authentication.	25
2.3.2 Methods used in Adaptive Authentication.	27
2.3.3 Model Evaluation Techniques.	28
2.3.4. Review of the technologies used in the behavioural authentication	29
2.4. Existing work	31
2.4.1. Existing system	31
2.4.2. Behaviour based adaptive authentication	32
2.4.3. User attributes based adaptive authentication	34
2.5. Comparisons on Adaptive Authentication system.	37
2.6. Chapter Synopsis	38
3. Chapter	39
3. The Methodology	39
3.1. Overview of the Chapter	39
3.2. Identification of Effective Methodologies	39
3.2.1. Identified methodology for the study	39
3.2.2. Technique adopted for management of the research study	40
3.3. Chapter Synopsis	41
4. Chapter	42

4. The Elicitation and Analysis	42
4.1. Overview of the chapter	42
4.2. Identifying the stakeholders	42
4.3. Practices for eliciting requirements	42
4.3.1. A research questionnaire	42
4.4. Analysis on the required Non-Functional factors	43
4.5. Synopsis of the chapter	44
5. Chapter	45
5. Professional Practices, Legal Considerations, Social and ethical related Issues	45
5.1. Overview of the chapter	45
5.2. Professional Practices, Legal Considerations, Social and ethical related Issues	45
5.3. Synopsis of the chapter	46
6. Chapter	47
6. Overall Design of the project and the Design Diagrams	47
6.1. Overview of the chapter	47
6.2. Motivation on the project design	47
6.3. A High Level of System Architecture	48
6.3.1. Layer of Presentation	51
6.3.2. Layer of Application	51
6.4. Component Diagram with the dataflow	52
6.5. Class Diagram	53
6.6. Sequence Diagrams for machine learning model process.	53
6.6.1. Retrieving the risk profile from machine Learning models	53
6.6.2. Diagram of the Sequence of Choosing the Second Factor Authentication.	54
6.7. The High-Level Architecture Flowchart Diagram for The Proposed Adaptive Authentication System	54
6.8. User Interface Wireframes	56
6.9. Chapter Synopsis	57
7. Chapter	58
7. The Implementation Methodology	58
7.1. Overview of the chapter	58
7.2. Effective tool and technology adoption	58
7.2.1. Stack of Tools and Technology	58
7.2.2. Choosing Suitable Programming Languages for implementation	59
7.2.3. Choosing appropriate libraries for Machine Learning Models	60
7.2.4. Selection of Integrated Development Environment (IDE)	60
7.3. Feature Selection for the implementation	60
7.4. Implementation of Core Functionality	62
7.4.1. Implementation of a Machine Learning Component	62
7.4.2. Adaptive Authentication Core Engine	63
7.4.3. Adaptive Authentication System Deployment	66
7.5. Difficulties encountered in the Implementation Methodology and the Solutions adopted	66
7.5. Chapter Synopsis	67
8. Chapter	68
8. The Overall Testing of the project	68
8.1. Overview of the chapter	68
8.2. System testing objectives	68
8.2.1. Testing on Functional requirements	69

8.2.2. Non-Functional Testing Results	71
8.2.3. Integration Testing	77
8.2.4. Model Validation	79
8.3. Comparisons with the industry standards	80
8.3.1. Comparisons with the traditional methods	81
8.3.2. Internal Comparisons	81
8.4. Chapter Synopsis	83
9. Chapter	84
9. Evaluation	84
9.1. Chapter Overview	84
9.2. Approach adopted to engage with evaluation process	84
9.3. Criteria for Evaluation	85
9.4. Evaluation evaluators	86
9.5. Evaluation Findings	88
9.5.1. What is the overall opinion about the project concept?	88
9.5.2. Comment on the depth of the project scope	90
9.5.3. What are your thoughts on the design, architecture, and implementation of the entire system?	93
9.5.4. Feedback on the demo prototype and the project solution	95
9.5.5. Critical analysis of the solution from the standpoint of its limits	97
9.6. Evaluation on Quantitative Approach	99
9.6.1. Complexity of the demo prototype and the solution implemented	99
9.6.2. Evaluation outcome on the UI/UX Experience	99
9.6.3. Evaluation on the comparison with the existing system	100
9.7. Functional Requirements Evaluation	100
9.8. Non-Functional Requirements Evaluation	104
9.9. Evaluating the entire project from the author's point of view	106
9.9.1. Novel techniques and their benefits throughout the project	108
9.9.2 Comparison with Existing System	109
9.10. Chapter Synopsis	109
10. Chapter	111
10. Project Conclusions and Future Recommendations	111
10.1. Overview of the Chapter	111
10.2. The importance of the aim and the emphasis on objectives	111
10.2.1. Achievement of the Study's aim	111
10.3 Making use of pre-existing skills and identity domain knowledge	111
10.4.1 Learning New Skills	113
10.5. Challenges and Obstacles	113
10.6 Future Improvements	114
10.7 Closing Remarks	115
References	117
Appendix	121
Appendix-1: The questionnaire for the evaluation process	121

LIST OF FIGURES

Figure 1 - Overall High-Level Architecture	50
Figure 2 - Component Diagram with the dataflow	52
Figure 3 - Class Diagram flow	53
Figure 4 - Sequence Diagram for the retrieval of the user risk profile	54
Figure 5 - Sequence diagram for choosing second authentication methods	54
Figure 6 - High-Level process with flowchart diagram	55
Figure 7 - Sign-Up UI wire frame	56
Figure 8 - Login UI wire frame	57
Figure 9 - JMeter Thread Group Configs for Load Test	72
Figure 10 - JMeter HTTP request Configs for Load Test	72
Figure 11- JMeter Performance Load Test	73
Figure 12 - CPU usage, memory, total thread count, total classes loaded during the load test	74
Figure 13 - CPU usage, memory, total thread count, total classes loaded during the load test for python engine	75
Figure 14 - CPU usage, memory, total thread count, total classes loaded during the load test for login application	76
Figure 15 - Web Application Performance	77
Figure 16 - Complexity of the demo prototype and the solution implemented	99
Figure 17 - Evaluation outcome on the UI/UX Experience	100
Figure 18 - Evaluation on the comparison with the existing system	100

LIST OF TABLES

Table 1.1 - Comparison between existing work on behaviour based adaptive authentication	8
Table 1.2 - Comparison between existing work on user context based adaptive authentication	10
Table 8.1 - Sign-Up Process Functional Testing	69
Table 8.2 - Login Process Functional Testing	70
Table 8.3 - Generic Flows Functional Testing	70
Table 8.4 – I&T Results	78
Table 8.5 - Machine learning model for user behavioral data	79
Table 8.6 - Machine learning model for user contextual data	80
Table 8.7 - Internal flow Comparisons	83
Table 9.1 - Criteria for Evaluation	86
Table 9.2 - Evaluator Affiliations	88
Table 9.3 - Overall opinion about the project concept	90
Table 9.4 - The depth of the project scope's critical evaluation	92
Table 9.5 – Opinion on the design, architecture, the system's implementation	95
Table 9.6 – Evaluation of the Implemented prototype and the solution provided	97
Table 9.7 - Critical analysis of the solution from the standpoint of its limits	98
Table 9.8 – Critical evaluation of Functional factors required	104
Table 9.9 – Critical Evaluation of Non-Functional factors required	106
Table 9.10 - Author's Evaluation on the whole project Evaluation Criteria	108

LIST OF ABBREVIATIONS

Abbreviation	Description
KNN	K-Nearest Neighbor
SVM	Support Vector Machine