

UNIVERSITY OF BAHRAIN

**College of
Information Technology**



**Department of
Computer Engineering**

A Fast and Adaptive Passwordless Multi-Factor Authentication Solution

A Thesis Submitted in Partial Fulfilment of the Requirements for the
M.Sc. Degree in Cybersecurity

Submitted by

Mohammed Aziz Al Kabir
202101768

Supervised by

Dr. Wael Elmedany
Associate Professor
University of Bahrain

May 2024



Dissertation Deposit Form

Author Name:	Mohammed Aziz Al Kabir		
Email:	202101768@stu.uob.edu.bh	Contact No:	34040796
College:	Information Technology		
Department:	Information Systems		
Thesis Title:	A Fast & Adaptive Passwordless Multi-Factor Authentication Solution		
Year:	2024		

Author's Declaration: I agree to the following conditions:

The above thesis will be available (in the University of Bahrain library and externally) and reproduced as necessary at the discretion of the University of Bahrain. It may also be digitized by the University of Bahrain and made available via the university's repository or via other parties on the Internet.

This condition shall apply to ALL copies including electronic copies.

The above thesis has been provided on the understanding that it is copyright protected material and that no quotation from this thesis may be published without proper acknowledgement.

Signature of the Author:	Mohammed Aziz Al Kabir	Date:	04-May-2024
--------------------------	------------------------	-------	-------------

DECLARATION

I declare that this work is the result of my own investigation and that it has not already been accepted in substance for any degree, nor is it currently submitted for any degree.

Signed: Date: 04/05/2024

Mohammed Aziz Al Kabir (Candidate)

The Thesis defense committee considers the thesis titled:

A Fast & Adaptive Passwordless Multi-Factor Authentication Solution

Submitted by Mohammed Aziz Al Kabir to the College of Information Technology is satisfactory and acceptable for the Master of Science in Cyber Security.

The Defense Committee:



Dr. Wael Elmedany
(Supervisor)

Department of Computer Engineering
University of Bahrain



Prof. Kevin Curran
(External Examiner)

Ulster University



Dr. Mohsen Rouached
(Internal Examiner)

Department of Computer Science
University of Bahrain

ABSTRACT

Passwords have always been inherently insecure, but their continued use and ubiquitous nature raises significant security concerns in today's ever-evolving digital landscape. This academic endeavour aims to explore the feasibility of a novel Adaptive Risk-based Passwordless Authentication (ARPA) scheme that combines the strengths of FIDO2 authentication and adaptive risk-based authentication. ARPA aims to tackle the growing need for a robust, secure, and user-friendly passwordless authentication solution by leveraging FIDO2's secure authentication protocols and dynamically adjusting security measures based on real-time risk analysis. The idea is to let an intended user access their account with little-to-no hindrance whilst a fraudulent user will either be challenged further or completely denied access to deter them from continuing with their malicious agenda. In the event that a non-negligible but not high enough risk is detected, users will be requested to re-authenticate themselves using a biometric or possession-based factor.

This thesis presents the design rationale behind the ARPA scheme by focusing on the challenges and opportunities of implementing such a scheme, particularly its technical and practical considerations as well as its demonstrable benefits and potential limitations in real-world applications. To assess its practical viability, a basic proof-of-concept version of the scheme was developed and tested with a group of volunteers. User feedback and data collected through close-ended survey questions provided valuable insights into the perceived usability, security, and effectiveness of the proposed user authentication scheme.

The findings herein demonstrate a promising passwordless authentication solution. The inherent 2FA/MFA nature of the scheme, coupled with its adaptive risk assessment capabilities that dynamically adjust security measures based on real-time user behaviour and contextual factors, offers a compelling approach to enhancing security and privacy without compromising user convenience as they can simply use their preferred biometric or possession-based sign-in method to access their favourite website without having to worry about account takeovers, password leaks or thefts, and data breaches. Users have the choice of using platform or external (roaming) authenticators to sign in, both of which can easily be the smartphone in their pocket without having to install any additional application.

The paper concludes by outlining a comprehensive scope of future work, including further refinement of the prototype, large-scale testing, and integration with real-world environments. This thesis paves the way for further exploration of ARPA as a viable, secure, and user-centric alternative to traditional password-based authentication methods that is well-suited for organisations of all sizes.

Contents

APPROVAL	A
DECLARATION	B
ABSTRACT	C
TABLE OF CONTENTS	D
LIST OF FIGURES	H
LIST OF TABLES	J
LIST OF ABBREVIATIONS	K
ACKNOWLEDGMENTS	L
DEDICATION	M
PUBLICATIONS	N
1 Introduction	1
1.1 Overview	1
1.2 Research Problem	2
1.3 Research Questions	5
1.4 Research Objectives	10
1.5 Contribution to the Field	11
1.6 Thesis Outline	12
2 Literature Review	14
2.1 Overview	14
2.2 Related Works	15
2.2.1 Going Passwordless with FIDO2	16

2.2.1.1	WebAuthn 2 API	17
2.2.1.2	CTAP 2.1 protocol	18
2.2.1.3	Inner workings of FIDO2	19
2.2.1.4	Benefits of implementing FIDO2	23
2.2.1.5	Limitations of FIDO2 and its barriers to entry	27
2.2.2	Improved Security and Usability with aRBA	32
2.2.2.1	Inner workings of aRBA	32
2.2.2.2	Overview of the factors typically used by aRBA	33
2.2.2.3	How risk scores are calculated	38
2.2.2.4	Categorisation of risks	40
2.2.2.5	Benefits of implementing aRBA	41
2.2.2.6	Limitations of aRBA and its barriers to widespread adoption	43
2.3	Discussion: Why combine the two?	45
3	Methodology	47
3.1	Overview	47
3.2	Research Design	48
3.3	Data Collection Methods	50
3.3.1	Prototype Development	50
3.3.1.1	Technology Stack	50
3.3.1.2	Technical Diagrams	52
3.3.1.3	Risk Score Calculation Model	60
3.3.1.4	Database Schema	62
3.3.1.5	Pseudocode	68
3.3.2	User Testing (Experimentation)	71
3.3.3	Survey Questionnaire	72
3.3.4	Ethical Considerations	73

3.4	Data Analysis	73
3.5	Research Limitations	73
4	Results and Discussion	75
4.1	Overview	75
4.2	Bridging the Gap	76
4.3	User Testing (Experimentation)	77
4.3.1	Overview	77
4.3.2	Prelude	77
4.3.3	User Registration Process	79
4.3.4	User Login Process	81
4.3.4.1	Baseline Logins	81
4.3.4.2	Testing Risk Scenarios	82
4.3.4.3	FIDO2 Re-authentication	85
4.3.4.4	Purpose of the Experiment	88
4.3.4.5	Post-experiment Survey	88
4.4	Discussion of Results	89
4.4.1	Survey Questions & User Responses	89
4.4.1.1	Baseline Questions	89
4.4.1.2	Targeted Questions	92
4.4.2	Mapping of Questions	100
4.4.3	Key Findings	102
4.5	Limitations	105
4.5.1	Limited Sample Size	105
4.5.2	Lack of Raw Performance Metrics	105
4.5.3	Lack of Open-Ended Questions	106
4.5.4	Lack of Behavioural Data	107
4.5.5	Partially Answered Research Questions	107
4.5.6	Potential for Overlooked Issues	108
4.6	Summary	108

5	Conclusion and Recommendations	114
5.1	Final Overview	114
5.1.1	Recap of ARPA’s Underlying Technologies	114
5.1.2	Conclusion	117
5.2	Recommendations	118
5.2.1	Build upon a Strong Foundation	118
5.2.2	Incorporate Machine Learning	119
5.2.3	Addressing Low Awareness and Adoption Rates	120
5.2.4	Opt for Self-Hosting	120
5.3	Future Work	121
	References	128
	Appendices	134
	Abstract (in Arabic)	144

List of Figures

2.1	A very high-level overview of the two components of FIDO2 in action.	17
2.2	An illustration of the inner workings of the FIDO2 authentication standard.	21
2.3	A sequence diagram of the FIDO2 registration flow.	22
2.4	A sequence diagram of the authentication (sign-in) flow using FIDO2.	22
2.5	Google’s hybrid signature approach offers a secure nesting of the standard ECC signature inside the Dilithium’s post-quantum cryptography (PQC) signature.	25
2.6	Implementation of an aRBA scheme dynamically responding to three different risk levels that indicate the likelihood of a fraudulent sign-in attempt and dynamically adapting the system’s authentication requirements as deemed appropriate.	33
2.7	Flowchart of how various factors are weighted in aRBA schemes to determine the risk of a fraudulent login attempt by calculating an aggregated risk score.	39
2.8	High-level overview of a typical aRBA system in action.	42
3.1	Simplified flowchart of the user registration flow in the proposed ARPA scheme.	52

3.2	Simplified flowchart of the user login flow in the proposed ARPA scheme.	53
3.3	Simplified illustration of the user registration process powered by FIDO2 in the proposed ARPA scheme.	54
3.4	Simplified illustration of the passwordless user login flow powered by FIDO2 in the proposed ARPA scheme.	55
3.5	Simplified internal logic of the risk analysis engine component of the proposed user authentication scheme to dynamically safeguard user accounts.	56
3.6	Factors used by the adaptive risk engine for scoring each login attempt to determine the identity of the intended user in the prototype version of the ARPA scheme.	59
3.7	Comparison of the proposed ARPA scheme with traditional passwords, PINs, and various 2FA/MFA methods.	62
4.1	A high-level overview of the login process in the proposed ARPA scheme.	78
4.2	An illustration of the use of a security key in the proposed ARPA scheme.	86
4.3	An illustration of the use of smartphones as a roaming authenticator in the proposed ARPA scheme.	86
4.4	A very simplified illustration of the login process in the proposed ARPA scheme.	113

List of Tables

2.1	An overview of the three main types of FIDO2 authenticators.	19
2.2	Types of encrypted information shared between RPs and FIDO2 authenticators.	20
3.1	Weighting of the most commonly used factors in the adaptive risk engine component of the proposed ARPA scheme.	58
4.1	A truncated summary of the actions taken by the proposed ARPA scheme captured during a segment of the experiment.	84
4.2	Non-exhaustive list of FIDO2 certified devices and fallback authentication methods supported by the proposed ARPA scheme.	87
4.3	Mapping between the research questions (RQs) and the questions in the survey (SQs) along with the status of each RQ. .	101
4.4	Summary of the most common responses received for 10 + 22 questions asked to a sample of 32 users of the ARPA scheme prototype following its testing.	102
4.5	Comparison of the ARPA scheme with popular user authentication schemes.	110

LIST OF ABBREVIATIONS

2FA	Two-Factor Authentication
API	Application Program Interface
aRBA*	Adaptive Risk-based Authentication
ARPA	Adaptive Risk-based Passwordless Authentication
CTAP	Client-to-Authenticator Protocol
FIDO2	Fast IDentity Online v2
MFA	Multi-Factor Authentication
MitM	Man-in-the-Middle
RBA	Risk-based Authentication
RP	Relying Party
RQ	Research Question
RTT	Round-Trip Time
SQ	Survey Question
TTFB	Time To First Byte
UX	User Experience
W3C	World Wide Web Consortium
WebAuthn	Web Authentication

* *aRBA is stylised this way to make it visibly different from ARPA and avoid any confusion.*

ACKNOWLEDGMENTS

I would like to thank my Supervisor, Dr. Wael Elmedany as well as Dr. Hessa Al-Junaid, Dr. Ahmed M. Zeki, Dr. Hesham Al-Ammal, Dr. Abdulla Ahmed Alasaadi, and a few other course instructors from the bottom of my heart for not only helping me reach my final semester as a postgraduate student at the University of Bahrain, but for also guiding and supporting me throughout this entire academic endeavour. I deeply appreciate all the help, advice, encouragement, and feedback they have provided to me on various occasions during my time at the university. I would also like to express my sincerest gratitude to my immediate family members and my closest friends for their unconditional love and support from the start until finish, and for believing in me at times even when I did not believe in myself. Needless to say, I would also like to thank the people who took part in the user testing phase of this endeavour. Lastly, I would like to thank you, the reader, for taking the time to read this thesis and for your interest in my work. I hope that it proves to be helpful or insightful to you in some way.

DEDICATION

To my Supervisor, Dr. Wael Elmedany for providing me with unparalleled support and guidance throughout this entire endeavour and for his patience as well as willingness to give several chances to improve the quality of work; to my father, mother, and sister for their unconditional love, support, and encouragement even though I can never reciprocate the same amount to them; to my dear friends H.E. Yusuf A. Khalil, Syed M. Raza, and Ms. Swathi P for being a source of encouragement and support throughout this entire endeavour; and finally, to another dear friend (and co-worker) of mine for being a great source of inspiration, courage, determination, delight, and positivity. I am glad that fate allowed me to meet someone like you, MJ. Thanks for everything. Wishing you all every success in life!

PUBLICATIONS

It may kindly be noted that a portion of this thesis cites information from an IEEE-published conference proceeding that features a paper that was previously authored by me under the supervision of Dr. Wael Elmedany.

M. A. Al Kabir and W. Elmedany, "An Overview of the Present and Future of User Authentication," in 2022 4th IEEE Middle East and North Africa COMMunications Conference (MENACOMM), IEEE, Dec. 2022, pp. 10–17. DOI: 10.1109/MENACOMM57252.2022.9998304.

URL: <https://ieeexplore.ieee.org/document/9998304>

This thesis also cites information from another paper of mine that was published by Taylor & Francis in the Journal of Cyber Security Technology last year in July. The publication of the paper was made possible through the guidance and support of Dr. Wael Elmedany as well as Dr. Mhd Saeed Sharif from the University of East London in the UK.

M. A. Al Kabir, W. Elmedany, M. S. Sharif, "Securing IoT Devices Against Emerging Security Threats: Challenges and Mitigation Techniques," in Journal of Cyber Security Technology 7, no. 2 (2023): pp. 1-25. DOI: 10.1080/23742917.2023.2228053.

URL: <https://www.tandfonline.com/doi/full/10.1080/23742917.2023.2228053>

Lastly, a journal article based on this thesis is currently under the peer review process. The preprint version is available for reading.

M. A. Al Kabir and W. Elmedany, "Adaptive Risk-Based Passwordless Authentication: A FIDO2 Integrated Approach for Enhanced Security and Usability," in Cybersecurity, Privacy, & Networks eJournal (2024). DOI: 10.2139/ssrn.4795401.

URL: <https://ssrn.com/abstract=4795401>

Chapter 1

Introduction

1.1 Overview

It is generally believed that the first use of passwords on computers as a means of preventing unauthorised access dates back to the early 1960s, but the very idea of using passwords or passphrases go as far back as the time of the ancient Roman Empire. In addition to being outdated, the combination of people and passwords have long been regarded as the weakest link in the chain when it comes to security due to the general public's seemingly innate tendency to use and reuse weak, leaked, and other poorly chosen easy-to-remember passwords that compromise the security of countless accounts and systems for the sake of convenience and memorability (Al Kabir & Elmedany, 2022).

As there are a multitude of research papers and news articles that already establish how and why passwords are such a lucrative target for cybercriminals, why they provide inadequate security, the threats that have shown the potential to effectively render them useless, and the subsequent risk this can pose to users' data, privacy, accounts, and systems, this thesis will primarily be attempting to put forward and explore the feasibility of an Adaptive Risk-based Passwordless Authentication (ARPA) scheme by weighing its pros and cons in addition to implementing a basic, working proof-of-concept

and have it tested by a small but respectable group of volunteers to record their feedback for assessing its viability as a potential candidate for finally deprecating the use of passwords in favour of an authentication scheme that ensures a good balance of security, privacy, and usability, in addition to being interoperable as well as scalable.

This paper therefore hypothesises that the mass adoption of passwordless authentication solutions that focus on biometric, possession, and location-based factors will finally allow us to bid adieu to passwords for good.

1.2 Research Problem

Password-based authentication schemes are the Achilles' heel of the security of information systems. In spite of their obvious flaws which make them inherently insecure, they are still prevalent in use today due to the relative ease and speed at which they can be implemented and deployed by developers without having to worry about incurring any extra overhead costs or added complexity for users. Today, even the most inexperienced users have grown accustomed to accessing their accounts, devices, and even entire systems by simply entering their login credentials (usernames and passwords). They also do not require any special or additional devices on either end, and such antiquated schemes also ensure the highest level of interoperability and backward compatibility due to their simple nature.

However, the prevalent use of passwords is bad and often frowned upon by cybersecurity specialists because they can easily be guessed, cracked, obtained, leaked, stolen, and even retrieved by attackers by simply combing through publicly available posts and other details to acquire personal information such as their dates of birth, nicknames, names of parents, pets, or significant others, and other commonly used passwords. Methods such as phishing, credential stuffing, social engineering, brute-forcing until the right

string of characters is found, dictionary and rule-based attacks, keylogging, deploying malware and exploiting unpatched vulnerabilities to retrieve passwords, and utilising social engineering techniques on unsuspecting victims are continued to be used by cybercriminals (Al Kabir & Elmedany, 2022). The advent of readily available tools that incorporate machine learning — specifically, pre-trained neural networks — and other technically impressive yet unnerving applications of artificial intelligence systems trained using an ever-expanding range of datasets containing millions, if not billions, of compromised passwords is making it even easier for threat actors to effectively render passwords useless by producing near-perfect password guessing AI models. Moreover, poor or inadequate password storage practices and lack of proper technical controls in systems and applications continue to be one of the contributing factors of data breaches and account takeovers to this day. Storing passwords using weak or broken cryptographic hashing functions, ineffective salting techniques that can be worked out with enough time and guessing attempts, or worse, in plaintext, can easily expose users' accounts and data to various forms of cyberattacks by making them a low-hanging fruit for threat actors.

Despite the obvious risks associated with the use of passwords, it seems that people, applications, and websites still continue to use them because they are quick and easy to implement as well as use, which makes them cost-effective and widely accepted. Biometric authentication techniques such as fingerprint scanning, facial recognition, and iris scanning are not new, but they are also not yet widely adopted for use outside of unlocking smartphones, laptops, safes, and homes with home security systems because they require specialised hardware and software support, which is often comparatively expensive and much harder to implement properly. Additionally, there are also privacy concerns associated with the use of biometric authentication as users may be hesitant to share their biometric data with third parties.

Furthermore, while there have been numerous attempts to augment as well as supplant the use of passwords over the years by providing alternative means of signing in using various single-, two-, and multi-factor authentication schemes for accessing devices and accounts, none of them have reached the same level of prevalence and general user acceptance as passwords. This is mainly due to the fact that most multi-factor authentication schemes are often viewed as cumbersome by design as they require additional steps or devices to verify a user's identity, thereby making the overall login process much longer and more complex, which most users find frustrating, tedious, or inconvenient. Moreover, if a user does not have access to the required device, service, or information when they are challenged with a two- or multi-factor challenge, then they would risk being locked out of their own account for failing the challenge. This can cause delays in accessing critical information or services in time, leading to frustration and hampering productivity. As a result, most people prefer to use and rely on simpler login methods like entering passwords, even if they are inherently less secure.

This necessitates the implementation of a quick and scalable multi-factor authentication scheme that achieves a balance between securing users' accounts against a wide range of cyber threats, maintaining their privacy, and ensuring ease-of-use whilst providing additional layers of security to drastically minimise the risk of account takeovers from occurring. A scheme that not only outweighs the perceived inconvenience of using most multi-factor authentication schemes, but is also easy to use and relatively cheaper to implement for developers, businesses, and other organisations.

1.3 Research Questions

As this endeavour sought to explore the feasibility of combining FIDO2 and aRBA technologies, the following set of research questions were methodically formulated for guiding this study to delve into the technical, practical, user experience, and security aspects of this proposed combination. The aim was to find answers to as many questions as possible.

1. Effectiveness Evaluation:

- **RQ:Eff[01]** — “How effective are FIDO2 and aRBA in providing a secure and convenient user authentication experience compared to traditional password-based authentication schemes?”

Assessing the effectiveness of FIDO2 and aRBA directly against password-based authentication schemes provide a clear understanding of the potential improvements offered by the proposed scheme terms of security and convenience.

- **RQ:Eff[02]** — “How effectively can ARPA improve the overall user experience and ensure a balance between heightened security, privacy, and user-friendliness?”

This question delves into the fundamental aspect of combining FIDO2’s strong authentication capabilities with adaptive risk-based authentication’s dynamic risk assessment. It aims to explore the optimal integration approach to achieve enhanced security, privacy, and usability.

2. Integration Challenges:

- **RQ:Int[01]** — “What are the technical challenges of integrating FIDO2 into an aRBA scheme?”

Investigating the integration challenges specific to combining FIDO2 and aRBA addresses would provide valuable insights into technical complexities and other potential hurdles that may have to be overcome for a successful implementation.

- **RQ:Int[02]** — “What are the technical challenges of integrating the proposed scheme into existing systems and applications, and how can these challenges be mitigated?”

Identifying and mitigating the technical challenges in integrating the proposed scheme into existing systems would ensure a smoother transition and better adoption, thereby contributing to the overall success of the implementation.

3. Privacy and Regulatory Compliance:

- **RQ:Pri[01]** — “How can users’ privacy and data protection be ensured in the proposed ARPA scheme?”

This question addresses the privacy considerations in the proposed user authentication scheme. It aims to explore privacy-preserving techniques and data protection measures to safeguard user information.

- **RQ:Pri[02]** — “How does the proposed authentication scheme align with existing data protection and privacy regulations?”

Ensuring alignment with data protection and privacy regulations is crucial for ethical and legal considerations. This question addresses the regulatory compliance aspect of ARPA to ensure that it meets established international standards to safeguard users’ privacy.

4. User Experience and Satisfaction:

- **RQ:Use[01]** — “How does the proposed ARPA scheme impact user experience and satisfaction compared to traditional password-based methods?”

Focusing on user experience and satisfaction provides insights into the human-centric aspects of the proposed passwordless multi-factor authentication scheme. Therefore, this question attempts to extrapolate how likely would people feel confident and convenient enough to use the proposed scheme over entering passwords as it offers a basis for understanding ARPA’s potential impact on user acceptance.

- **RQ:Use[02]** — “What are users’ general perception and attitude towards the proposed authentication scheme?”

Once again, understanding users’ perception and attitude provides valuable qualitative data, which can then be used to gauge the acceptability of the proposed user authentication scheme in the eyes of end-users.

5. Security Evaluation:

- **RQ:Sec[01]** — “How does the combined use of FIDO2 and aRBA improve the overall security of a system? What are the potential security enhancements achievable through this combination, particularly in comparison to traditional authentication methods?”

Investigating the potential synergies between FIDO2 and aRBA for security enhancements allow for a detailed analysis of how the combination contributes to overall system security, especially when compared to traditional methods such as entering passwords.

- **RQ:Sec[02]** — “What are the potential security vulnerabilities and attack vectors introduced by the combination of FIDO2 and aRBA in the proposed passwordless multi-factor authentication scheme, and how can they be mitigated?”

This question focuses on identifying and addressing security risks arising from the integration of FIDO2 and aRBA. It aims to assess the potential vulnerabilities and develop mitigation strategies to ensure the scheme’s robustness against cyberattacks.

6. Scalability and Performance:

- **RQ:Sca[01]** — “How would the proposed scheme perform in terms of scalability, especially in systems with a large userbase?”

As scalability is crucial for practical implementations, this question attempts to gauge the performance, reliance, and viability of the proposed scheme in real-world scenarios with a large userbase.

- **RQ:Sca[02]** — “What are the resource requirements and performance implications of implementing FIDO2 into an aRBA scheme in terms of authentication latency, throughput, and resource utilisation?”

This question focuses on evaluating the performance impact of the integrated authentication scheme. It aims to assess the effect on authentication speed, transaction processing capacity, and system resource consumption.

7. User Adoption and Education:

- **RQ:Ado[01]** — “What are the barriers to user adoption of the proposed user authentication scheme, and how can they be overcome?”

Identifying the main barriers to widespread adoption is crucial for developing targeted strategies to overcome resistance and facilitate a smoother transition and integration of the proposed authentication scheme.

- **RQ:Ado[02]** — “What strategies are effective in educating users about FIDO2-based passwordless authentication schemes as well as aRBA, and how would raising awareness or education impact user adoption?”

Understanding and implementing effective strategies for user education is key to fostering user adoption. This question addresses the educational aspect, providing insights into how awareness and education impact user acceptance of a new product or service.

8. Long-Term Viability and Future Trends:

- **RQ:Via[01]** — “How sustainable is the proposed passwordless authentication scheme in the long term, considering emerging technologies and cyber threats?”

Assessing the long-term sustainability of the proposed scheme considers its adaptability to emerging technologies and evolving cyber threats, thereby ensuring its relevance over an extended period of time.

- **RQ:Via[02]** — “What future trends in authentication methods might impact the continued relevance of the proposed user authentication scheme?”

Anticipating future trends would allow for proactive adjustments to be made to the proposed ARPA scheme for ensuring that it remains at the forefront of technological advancements in the dynamic field of cybersecurity and evolving threats.

9. Comparative Analysis:

- **RQ:Ana[01]** — “How does the proposed passwordless authentication scheme compare with existing as well as other emerging authentication methods?”

A comparative analysis provides a comprehensive evaluation of the proposed user authentication scheme and its overall suitability based on its security, usability, and adoption rates in comparison to existing and emerging user authentication methods.

- **RQ:Ana[02]** — “How can ARPA be optimised to take full advantage of FIDO2 and aRBA’s strengths whilst simultaneously addressing most, if not all, of their respective limitations by combining the two?”

This question ponders the strategies that may be adopted to maximise the effectiveness of integrating FIDO2 into an aRBA-based passwordless authentication scheme. It aims to identify areas where aRBA can compensate for FIDO2’s shortcomings and vice versa for enhancing the overall level of security, privacy, and usability of the proposed user authentication scheme.

1.4 Research Objectives

The primary objectives of the work in this thesis are summarised as follows:

1. Ascertain the feasibility of an Adaptive Risk-based Passwordless Authentication (ARPA) scheme to supplant traditional or static knowledge-based and multi-factor authentication (MFA) schemes by addressing most, if not all, the issues that plague such schemes.

2. Explore the practicality of adopting Adaptive Risk-based Authentication (aRBA) to score every login attempt for determining its authenticity by assessing one or more preset factors.
3. Delve into the viability of having the protection offered by MFA schemes but none of its inconveniences or security and privacy-related concerns by incorporating the FIDO2 open authentication standard into an aRBA scheme or model.
4. Develop a basic, working proof-of-concept version of the proposed solution.

1.5 Contribution to the Field

The primary contribution of this endeavour is to lay down the foundation of a novel and innovative multi-factor user authentication scheme that aims to provide an optimal balance of users' security, privacy, and usability by automatically determining if a login attempt is valid or fraudulent with a relatively high accuracy based on certain criteria. This is achieved by developing a scheme that essentially combines the FIDO2 open authentication standard and Adaptive Risk-based Authentication (aRBA) to eliminate the use of passwords in favour of other user authentication factors such as location, possession, and biometric identification. The scheme also takes users' privacy into consideration as much of the processing will be done locally on their devices, and any outgoing information will be hashed before being transmitted to a web server or database. Moreover, all biometric and other personal information will be encrypted prior to being locally stored on the user's device with policies being set that limit what data, even if encrypted, leaves a user's device.

Facilitating the long-pending matter of finally deprecating the use of passwords altogether would certainly be a major contribution in a world where everything is seemingly becoming digital and interconnected. Thus, having a user-friendly authentication scheme that ensures better privacy whilst simultaneously providing increased protection against a myriad of cyber threats that plague pin- or password-based authentication schemes would be an ideal candidate for replacing knowledge-based authentication methods for good. The last thing this world needs is a flawed and antiquated user authentication mechanism that provides inadequate account security and is constantly a lucrative target for cybercriminals worldwide.

1.6 Thesis Outline

The structure and content of each chapter in this thesis will guide readers through a comprehensive exploration of the topic at hand — exploring the feasibility of the Adaptive Risk-based Passwordless Authentication (ARPA) scheme with the aim to deprecate the use of passwords for good.

- As established so far, **Chapter 1** serves as the introduction by providing an overview of the research problem, the significance of the problem, the research questions that this endeavour attempts to answer, and the objectives of the thesis. It sets the stage for subsequent chapters by presenting the context and rationale for the research. Each chapter hereafter serves a distinct purpose, contributing to the overall understanding and advancement of knowledge in the field of user authentication, particularly FIDO2 passwordless authentication and aRBA.

- **Chapter 2**, which comprises the literature review section of this thesis, delves into the inner workings of the FIDO2 open authentication standard and aRBA in great detail. It critically analyses and synthesises existing studies, theories, and frameworks relevant to the research topic to offer a comprehensive understanding of the current state of knowledge in the field and identifying gaps that this thesis aims to address.
- **Chapter 3** puts forward a basic but novel proof-of-concept of a user authentication scheme that attempts to incorporate the FIDO2/WebAuthn protocols into an aRBA scheme. It also focuses on the methodology employed in the thesis by detailing the research design, data collection methods, and data analysis techniques that were utilised to gather and analyse relevant information.
- In **Chapter 4**, the strengths and limitations of the proposed ARPA scheme as well as the design of the study are discussed in great detail by drawing attention to the key findings and results obtained in a clear and concise manner, supported by appropriate visual aids such as tables and figures. The presented findings are then analysed and interpreted in light of the research objectives, comparing them with existing user authentication schemes and offering insights into the implications of using the proposed ARPA scheme.
- And finally, **Chapter 5** brings the thesis to a conclusion by summarising the key findings, discussing their implications, and highlighting the contributions made to the field. Moreover, this chapter also identifies areas for future research and suggests potential improvements or extensions to the current work. It offers a sense of closure while also presenting opportunities for further exploration and development in the field of passwordless authentication.

Chapter 2

Literature Review

2.1 Overview

As passwords and most other traditional user authentication schemes are becoming increasingly vulnerable to a variety of ever-evolving cyberattacks such as — but certainly not limited to — phishing, guessing, credential stuffing, spraying, intercepted then replayed, brute-forced, and even guessed, there is a growing need for more secure authentication schemes that are not only easy to use for the vast majority of people, but can also respect their privacy as well (Al Kabir & Elmedany, 2022; Kabir, Elmedany, & Sharif, 2023).

One such contender is the Adaptive Risk-based Authentication (aRBA), but this scheme by itself cannot adequately offer the best balance of security, privacy, and usability as this chapter will later explore. Another promising candidate is the open authentication standard called FIDO2, which is designed to replace passwords with more secure authentication methods such

as biometrics and security keys by utilising commonly used devices such as users' smartphones and laptops for seamless authentication to online services across mobile as well as desktop environments.

By thoroughly examining existing literature, this chapter aims to provide a comprehensive understanding of the theoretical foundations, practical implementations, and potential challenges associated with FIDO2 and aRBA. Through an in-depth analysis of previous studies, standards, and frameworks, this chapter seeks to identify gaps in the current research landscape and lay the groundwork for the development of an innovative multi-factor user authentication scheme that utilises the strengths of both FIDO2 and aRBA by essentially combining them.

2.2 Related Works

The proposed multi-factor user authentication scheme represents an innovative approach by combining the characteristics and strengths of FIDO2 and aRBA. This unique amalgamation aims to enhance the security and usability of user authentication processes whilst ensuring a commendable level of privacy. However, the novelty of this scheme presents a challenge in terms of drawing comparisons or establishing similarities with existing schemes. Extensive research conducted in both real-world implementations and academic literature has revealed a lack of similar schemes that integrate FIDO2 into an aRBA scheme. Though there are a number of papers that discuss the two technologies separately, none of them explicitly address the combination of the two and its feasibility. Consequently, the absence of comparable schemes underscores the originality and potential ground-breaking nature of the proposed multi-factor user authentication scheme, thereby necessitating a comprehensive exploration and evaluation of its feasibility, effectiveness, and potential limitations.

Therefore, this chapter will be delving into the two core components of the proposed multi-factor authentication scheme and then discuss how they can theoretically work in tandem to offer an optimum balance of security, privacy, and usability for users.

2.2.1 Going Passwordless with FIDO2

Short for Fast IDentity Online v2, FIDO2 is a relatively modern open standard for passwordless authentication that aims to provide enhanced security, privacy, and user experience by leveraging public-key cryptography to create strong, tamper-resistant authentication credentials and biometric verification, inter alia, to eliminate the over-reliance on passwords and other traditional knowledge-based authentication schemes (Bindel, Cremers, & Zhao, 2023; Alqubaisi, Wazan, Ahmad, & Chadwick, 2020).

Initially released in 2018, FIDO2 builds on top of the FIDO Alliance's previous work, namely the Universal Authentication Framework (UAF) and the Universal 2nd Factor (U2F) protocols, which laid the foundation for passwordless authentication when they were released in 2014 to complement existing two-factor authentication (2FA) solutions as open authentication standards that could be adopted to provide an extra layer of security online (Barbosa, Boldyreva, Chen, & Warinschi, 2021), (Rasmussen, 2021), (Ranise, Sciarretta, & Tomasi, 2020).

The FIDO2 standard primarily consists of two main components, the WebAuthn 2 API and the CTAP 2.1 protocol, each serving distinct but complementary purposes to allow strong, passwordless, and phishing-resistant user authentication to take place in a robust and user-friendly manner, as illustrated in Figure 2.1.

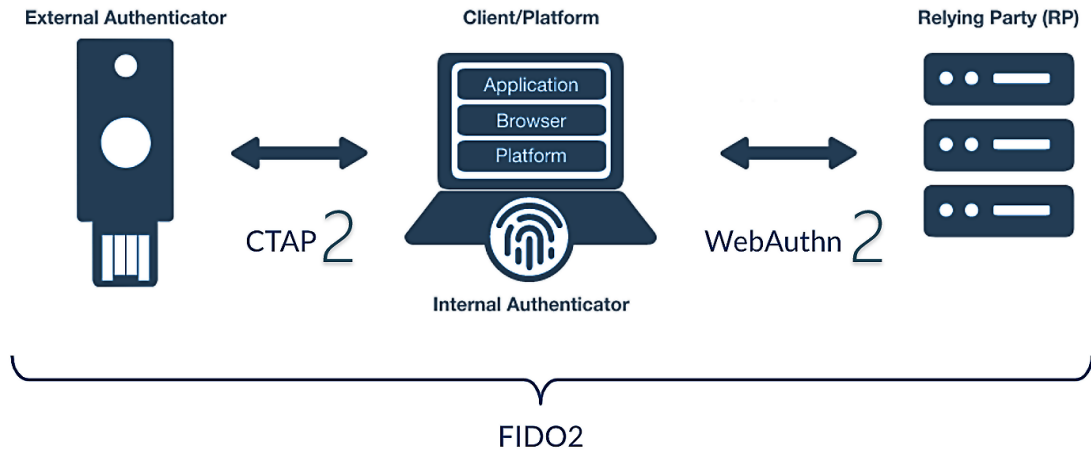


Figure 2.1: A very high-level overview of the two components of FIDO2 in action.

2.2.1.1 WebAuthn 2 API

Currently in Level (or version) 2 and written in JavaScript, the Web Authentication (WebAuthn) API is an extension of the Credentials Management API developed by the World Wide Web Consortium (W3C) in conjunction with the FIDO Alliance. It was developed to sit between web applications, W3C-compliant web browsers, and authenticators for generating unique pairs of private and public keys in the browser itself using the device’s Trusted Execution Environment (TEE) or Trusted Platform Module (TPM) and then stored locally in the authenticator for allowing web applications to register and authenticate users with biometrics, security keys, and trusted devices as opposed to using shared secrets like passwords (Farke, Lorenz, Schnitzler, Markert, & Dürmuth, 2020).

At its core, the WebAuthn API allows a web application (known as Relying Party or RP) to perform a passwordless challenge-response authentication with a specific authenticator — where the web browser acts as an intermediary — and the responses are signed by private keys, which the RP (web server) then verifies using the corresponding public key and subsequently takes whatever action is deemed necessary (Lassak, Hildebrandt, Golla, & Ur, 2021). This process is known as “attestation” and it ensures that only

the authenticator possessing a user’s private key can successfully authenticate that user (Mašek & Novotný, 2022). FIDO2-enabled devices generate a new pair of keys for each RP during the registration process. The pairs are then used in subsequent authentication and re-authentication processes.

The newer version or level of the WebAuthn API supports a wider range of authenticator types for allowing users to choose from a range of options based on their preferences or device capabilities and it also includes a number of security improvements over the original version, notably the introduction of automatic enrollment of authenticators to make it easier for users to enroll their authenticators using QR codes or NFC tags and credential binding to ensure that a credential can only be used to authenticate to a web application if it is presented by the correct authenticator, thereby combatting credential theft (Bindel et al., 2023). Moreover, the WebAuthn API also uses CTAP (discussed next) to communicate with authenticators during registration, authentication, and re-authentication processes. The previously mentioned authors Bindel et al. even went so far as to prove post-quantum security for FIDO2 with WebAuthn 2 and CTAP 2.1 under certain conditions with minor protocol extensions put forward by them.

2.2.1.2 CTAP 2.1 protocol

CTAP 2.1, or Client-to-Authenticator Protocol v2.1, is a platform-independent application layer protocol that defines how clients such as web browsers communicate with authenticators like security keys or biometric devices during registration, authentication, and re-authentication by facilitating the secure exchange of information during each process (Lassak et al., 2021).

In addition to having cross-platform support to offer interoperability across different clients (web browsers), devices, and operating systems, CTAP 2.1 also allows for device enumeration — which in turn allows clients to identify and communicate with multiple authenticators linked to the user’s device

(Bindel et al., 2023). This gives users the choice of having multiple authenticators to serve as backups in case one fails, becomes lost, or is not currently on their person (Ghorbani Lyastani, Schilling, Neumayr, Backes, & Bugiel, 2020).

Moreover, CTAP 2.1 also supports token binding to vastly minimise authentication token replay attacks by making it harder to intercept and reuse tokens as each authentication token gets bound to a specific client, which means that the token can only be used to authenticate to a web application if it is presented by the correct client (Bindel et al., 2023; Vasileios Grammatopoulos, Politis, & Xenakis, 2021).

2.2.1.3 Inner workings of FIDO2

Other than the WebAuthn API and CTAP, authenticators are what allows a user to verify his or her identity to a FIDO2 passwordless challenge using their biometrics information or the use of physical tokens and software-based authenticators such as security keys and authentication apps respectively (possession-based factor). The table below classifies the types of authenticators and gives a brief description for each of them with examples.

Table 2.1: An overview of the three main types of FIDO2 authenticators.

Type	Description	Examples
Internal (platform)	The built-in authenticators are hardware-based and embedded directly into the device’s hardware. They offer strong security and user convenience, as the user’s biometric data is stored locally which makes them resistant to phishing and most MitM attacks due to local authentication.	Biometric sensors in smartphones and laptops (for fingerprint, palm, voice, facial, iris or retinal data), Windows Hello in supported Windows 10 and 11 machines, and Passkeys (that use Face ID and Touch ID) in supported Apple devices.
External (roaming)	Roaming authenticators are separate, platform-agnostic hardware devices that provide a high level of security and can be used across multiple devices. They are also resistant to phishing as they require the physical presence of a user to authenticate.	USB security keys (like YubiKey and Google Titan), NFC tokens (smart cards and tags), smartphones, smartwatches, SIM cards, and few other Bluetooth-enabled devices.

(continued next page)

Software-based	Software-based authenticators are applications that run on devices like smartphones for generating one-time passcodes (OTP) that are often time-based for authentication. While convenient, they are considered less secure than hardware-based options as they are susceptible to malware infection and device compromise.	Google Authenticator, Authy, Microsoft Authenticator, LastPass Authenticator, and Duo Mobile.
----------------	---	---

The FIDO2 authentication standard outlines and creates the environment for these authenticators to directly communicate with W3C-compliant web browsers or other WebAuthn client applications over USB-Human Interface Device (USB-HID), Bluetooth Low Energy (BLE), Near Field Communication (NFC), and Radio-Frequency Identification (RFID) for the back and forth sharing of encrypted information between relying parties (RPs) and FIDO2 authenticators (Ghorbani Lyastani et al., 2020), (Lassak et al., 2021). Table 2.2 enumerates the types of information that is typically shared between both sides. This is crucial as it provides a peek into the intricate inner workings of the FIDO2 registration and authentication flows.

Table 2.2: Types of encrypted information shared between RPs and FIDO2 authenticators.

Type	Description
Metadata and Attestation	Authenticators provide attestation information and other additional data (metadata) to RPs that mentions the details about the authenticator’s characteristics, capabilities, and origin. This information is then used by the RP to assess the security level and trustworthiness of the authenticator.
Public Key Credential (PKC) Request	During the sign-up or registration process, the RP sends a request to the authenticator for generating a unique pair of asymmetric keys by specifying the type of cryptographic algorithm to be used and other parameters for the key pair generation process. The corresponding public key is then shared with the RP.
Challenge	The RP sends a random challenge to the authenticator, which is a unique value that it must sign with the user’s private key after their explicit consent in order to prove the device’s possession.
Assertion (Challenge Response)	The authenticator generates an assertion in response, which includes the signed challenge value along with other information like the authenticator’s public key and a signature over the combination of these elements. It serves as proof of possession of the specific authenticator and the user’s authorisation of a login attempt.
User Verification (UV) Method	If an authentication process requires the user’s identity verification, then the RP will send a request to the authenticator for initiating the verification process. This typically involves providing a biometric sample, security token (card or tag) possession, or a PIN-related request.
Session Information	Certain implementations of FIDO2 involve the logging and sharing of session-specific information to maintain context and security throughout the authentication process.
Status and Error Messages	Various status and error messages may be exchanged between the relying party and the authenticator to communicate the outcome of the authentication process or any issues that may have occurred.

This open authentication standard is therefore comprised of four main elements — relying parties, FIDO2 authenticators, clients (like W3C-compliant web browsers), and of course, users. However, the actions of users are typically implicit in the description of the authenticator (Bindel et al., 2023).

As illustrated in Figure 2.2, these four main elements primarily communicate with one another with the aid of WebAuthn 2 API and CTAP 2.1 protocol, where the two work in tandem to allow for a passwordless challenge-response scheme between a FIDO2-compliant web application as well as its server (often referred to as "Relying Party" or RP) and a user respectively (Farke et al., 2020).

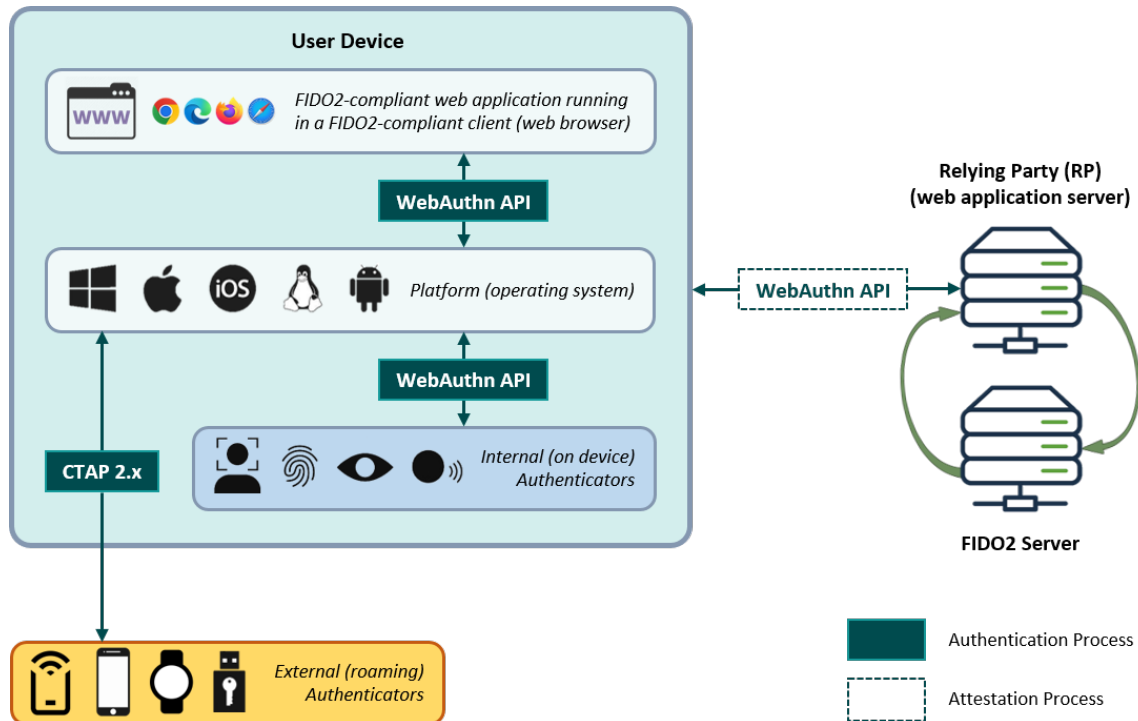


Figure 2.2: An illustration of the inner workings of the FIDO2 authentication standard.

FIDO2 focuses on minimising the amount of sensitive information that is exchanged during the user authentication process. The user's actual private key never leaves his or her authenticator device, and the information shared between parties is designed to prove possession of the private key without revealing the key itself. As the unique pairs of keys are mathematically re-

lated, each pair is assigned or bound to the identity of a specific user with a particular web application or RP during registration using a process called identity binding (Vasileios Grammatopoulos et al., 2021), (Klieme, Wilke, van Dornick, & Meinel, 2020). This enhances security and privacy while also allowing for a much stronger user authentication process as it allows websites and applications to bind a user’s identity to a specific authenticator. The flow of the registration as well as authentication process are shown in Figures 2.3 and 2.4 below.

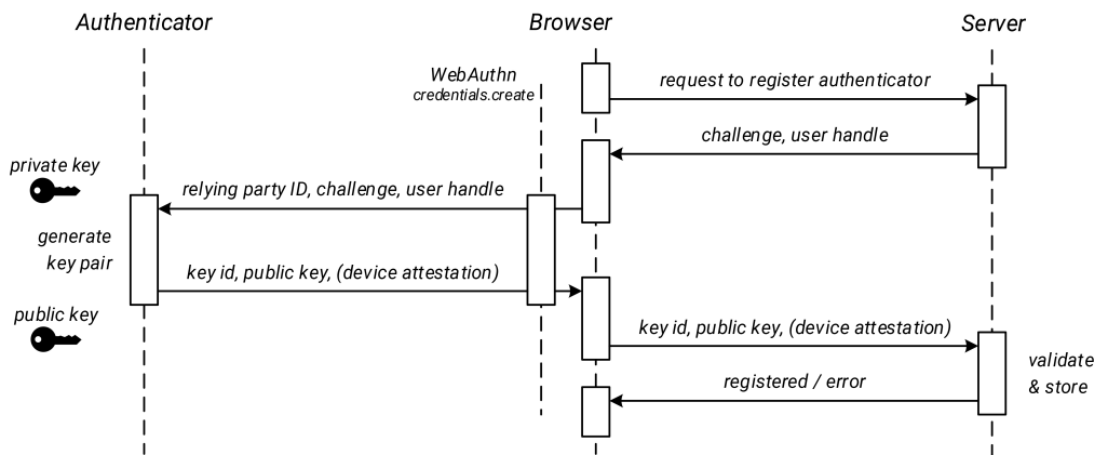


Figure 2.3: A sequence diagram of the FIDO2 registration flow.

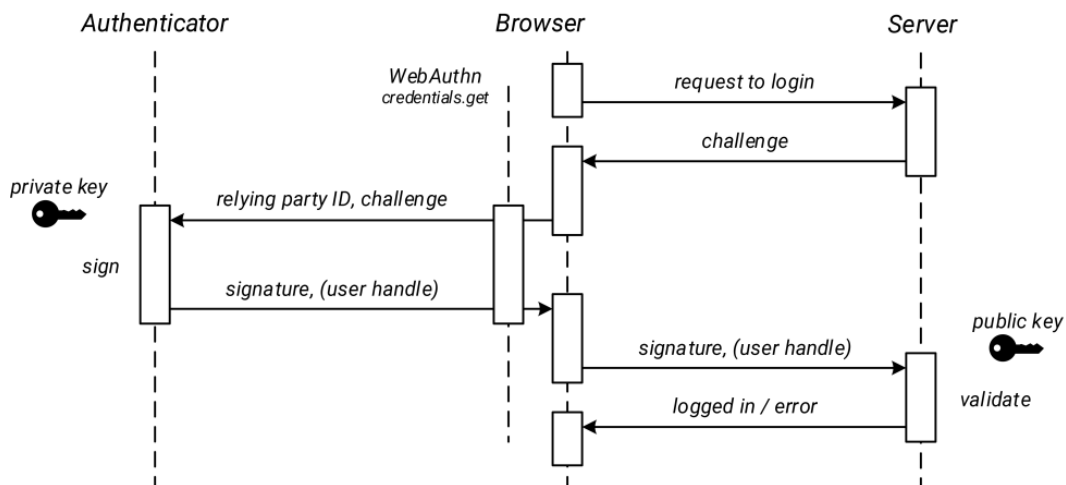


Figure 2.4: A sequence diagram of the authentication (sign-in) flow using FIDO2.

Moreover, each authenticator undergoes a device attestation process each time to verify its integrity and ensure its security by proving that it has not been tampered or compromised by unauthorised entities. This attestation is typically achieved through cryptographic measures, where the device in question proves its authenticity and integrity to the RP by providing verifiable evidence that is difficult to counterfeited (Alam, Krombholz, & Bugiel, 2019).

Lastly, the FIDO2 standard necessitates the use of Elliptic Curve Cryptography (ECC) for creating and verifying digital signatures that is mathematically linked to the data being signed for device attestation as well as challenge-response authentication (FIDO Alliance, 2021). This ensures that the signature can only be created by the entity that possesses the private key.

2.2.1.4 Benefits of implementing FIDO2

FIDO2 offers a modern open standard for passwordless authentication with enhanced security, privacy protection, seamless user experience, and interoperability. By leveraging public-key cryptography and eliminating the reliance on traditional passwords, FIDO2 significantly reduces the risk of password-related cyberattacks such as phishing and credential stuffing. It also prioritises user privacy by decentralising authentication credentials and isolating user identities, thereby reducing the risk of identity theft.

Moreover, FIDO2 provides a convenient and user-friendly authentication experience which eliminates the need for users to set weak or repeating passwords, remember multiple complex passwords, or be forced to use password managers, which are often susceptible to attacks by bad actors as their nature make them a very lucrative target.

With its open standard and guaranteed interoperability, FIDO2 ensures consistent, reliable, and easy-to-use passwordless authentication across various platforms, devices, and services.

Some of the other notable benefits of implementing FIDO2 are listed below.

- **Strong backing from industry leaders:** In addition to being backed by the W3C, the standard is also receiving direct support and contribution from the “Big Five” tech giants Google, Apple, Microsoft, Meta, and Amazon in addition to several other members of the FIDO Alliance like Intel, Samsung, Arm, Qualcomm, Huawei, Yubico, Nok Nok, Akamai, IBM Security, Red Hat, PayPal, MasterCard, Visa, American Express, Mozilla, VMware and many others (FIDO Alliance, 2022), (Barbosa et al., 2021).
- **Growing adoption and support:** FIDO2 is fully supported by Microsoft’s Windows 10 and 11 operating systems via Windows Hello biometric authentication system, Apple’s Touch and Face ID systems in iOS, iPadOS and macOS as well as Google’s Android operating system with their separate but FIDO2-compliant implementation of passkeys, and across all popular W3C-compliant web browsers, including Chrome, Edge, Safari and Firefox by dint of the W3C-backed WebAuthn specification (Ghorbani Lyastani et al., 2020), (Rasmussen, 2021), (Owens, Anise, Krauss, & Ur, 2021). As an added convenience, smartphones and smartwatches have the ability to automatically sign in users based on close proximity to their authenticators (trusted device or security tokens) using Bluetooth, GPS, and RFID with minimal or no interaction from the users’ side.

Furthermore, several popular websites and social media sites such as Google apps (YouTube, Gmail, Google Cloud, and so forth), Microsoft apps (like Azure, Office 365, Outlook, Teams, and Skype), Facebook, X (Twitter), GitHub, Amazon AWS, Yahoo, Cloudflare, eBay, Shopify and many others have already started to offer FIDO2-based authentication as an alternative to using passwords.

- **Quantum resilience:** The FIDO Alliance deprecated the use of Elliptic Curve based Direct Anonymous Attestation (ECDAA) in FIDO2 schemes earlier this year due to the discovery of a few security deficits and because it is not quantum resistant (Bindel et al., 2023). ECDAA has been superseded by Elliptic Curve Digital Signature Algorithm (ECDSA), which is a quantum resistant digital signature algorithm that is also more efficient than ECDAA, meaning that it can be used on devices with limited resources such as smartphones and even IoT devices. As a result, ECDSA is now the preferred signature algorithm for FIDO2 (FIDO Alliance, 2021).

As of August 2023, Google, a FIDO Alliance member, is putting forward a hybrid signature schema that builds on the standard array of security provided by the ECDSA signature algorithm by encapsulating it with the recently standardised quantum resistant signature algorithm, Dilithium (Bursztein & Kaczmarczyk, 2023). They are now in the process of implementing this novel ECC/Dilithium approach into their open source firmware for FIDO2 security keys called OpenSK. This hybrid signature schema can offer both ECC's protection against the standard set of attacks and Dilithium's resilience against quantum attacks, as illustrated in the figure below.

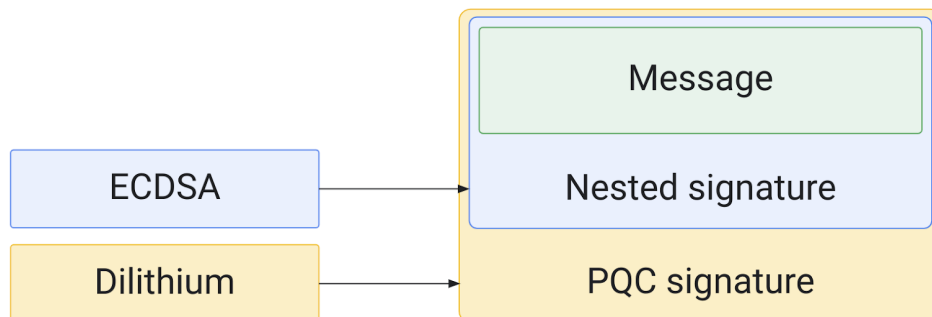


Figure 2.5: Google's hybrid signature approach offers a secure nesting of the standard ECC signature inside the Dilithium's post-quantum cryptography (PQC) signature.

- **No shared secrets:** Traditional authentication methods require both the user and the web application to know a shared secret (the password). This shared secret can be cracked or stolen and leaked, thereby compromising security. FIDO2 eliminates the need for shared secrets and alleviates password fatigue as the user's private key remains within the authenticator and the public key is registered with the service provider (RP). The user only needs to prove possession of their private key to authenticate. Moreover, unique pairs of keys are generated during each registration process.
- **Protection against phishing and replay attacks:** Traditional passwords are susceptible to phishing, but FIDO2 eliminates this risk by ensuring that authentication challenges are presented only to the legitimate website that the user intends to sign in to. Moreover, FIDO2 uses a cryptographic nonce for each authentication request to deter the interception and reuse of authentication data in replay attacks.
- **Standardisation and Interoperability:** The standardisation of this open authentication standard ensures interoperability among different authenticators and service providers (RPs) to promote its widespread adoption and reducing vendor lock-in. This allows it to work across various platforms and devices, including laptops, desktops, smartphones, and IoT devices. It also supports various communication methods such as USB-HID, NFC, Bluetooth, and platform-specific biometric sensors.

Moreover, web developers can implement FIDO2 into their web applications by using the previously mentioned WebAuthn API, which provides a standardised way for web applications to interact with FIDO2 devices.

2.2.1.5 Limitations of FIDO2 and its barriers to entry

While FIDO2 offers numerous benefits, including enhanced security and user experience, it is essential to recognise that it is not without limitations. Additionally, there are certain barriers to entry that organisations and users may face when adopting FIDO2.

- **Costly implementation:** Conforming to the FIDO2 authentication standard will require additional expenses to be incurred as the entire registration as well as sign-in flows will have to be reworked, which could be a slow and costly process with a potentially long system unavailability during the transition period.

Furthermore, there is no quick and easy way for organisations to set up and deploy security tokens — be it hardware or software — at a large scale for their employees. In this case, performing a trial run such as doing a limited beta testing and then gradually inviting more users to join could be a viable strategy. Users will also require sufficient training, so that they can feel comfortable using a different way of authenticating themselves on a regular basis.

As mentioned previously, organisations will need to invest in updating their systems to support FIDO2 and users must have devices that are FIDO2-compliant. This could pose a logistical challenge, especially for enterprises with legacy systems. Incompatibility between devices and services could lead to a fragmented user experience and deter users from embracing FIDO2.

- **Initial setup complexity:** The initial setup of FIDO2 authentication requires users to register their authenticator devices with online services (RPs) by verifying their identities using biometric and/or possession-based authentication. This process can be rather complex for users who are not technologically savvy, potentially discouraging the adop-

tion of passwordless authentication schemes, especially among older population.

- **Resistance to change:** Introducing a new authentication method will almost certainly require users to learn and adapt to the new process. As a result, FIDO2 might understandably pose a steep learning curve for users who are accustomed to traditional password-based authentication and this may lead to a slower user adoption rate due to the initial resistance or hesitation to adopt a new technology because of its perceived complexity or unfamiliarity. However, this may not be a significant psychological barrier for most users as they have already gotten used to unlocking their smartphones (and to a lesser extent, even laptops) with biometric authentication.
- **Misconceptions about FIDO2:** Most misconceptions about FIDO2, particularly the apparent distrust of biometric-based authentication systems in general stem from the general population's lack of knowledge and experience from using FIDO2-enabled devices (authenticators) and compliant systems. For instance, when asked by (Lassak et al., 2021), many people naturally assumed that their biometric information was being shared with — and stored in — servers/RPs or even third-party site, even though this assumption could not be further from the truth.
- **Increased device dependency:** FIDO2 authentication heavily relies on external authenticator devices such as security keys or biometric sensors. This device dependency can be a limitation in certain scenarios where users do not have access to their authenticators or when their trusted devices are lost, stolen, or malfunctioning. Such situations could lead to authentication challenges, potentially resulting in users being locked out of their own accounts.

- **Availability concerns:** There seems to be a reasonable fear of temporarily (or even permanently) losing access to a system or an account in the event of a power loss or a dead battery of an authenticator, abrupt disconnection from the Internet, and the loss, theft or deprecation of a trusted device to name a few (Owens et al., 2021). Many authenticators come with the option of setting up a backup PIN code for such an occasion, however the FIDO2 standard does not currently specify any appropriate or standard fallback authentication schemes for use in case the primary means of authenticating a user is unavailable. Building awareness about such fallback mechanisms must also be performed to not cause any panic and subsequent drop in the productivity or use of a particular FIDO2-compliant system (Kunke, Wiefling, Ullmann, & Iacono, 2021).
- **Pitfalls of hardware and software tokens:** Both hardware and software tokens have their own vulnerabilities. A software token can be compromised, modified, or accessed without authorisation if there are flaws in its implementation. On the other hand, a hardware token cannot be patched or updated when a security vulnerability is found. They can also be expensive for organisations to procure and distribute to their workforce. Additionally, employees may also find it inconvenient to carry around yet another device and risk losing or damaging it. Fortunately, modern smartphones can be used as roaming authenticators, and most people today have grown accustomed to using them.
- **Biometric vulnerabilities:** Biometric authentication, while convenient, is not immune to vulnerabilities and exploitation. Biometric data can be stolen or spoofed (forged), raising concerns about privacy and security. However, malicious actors will also have to steal or compromise the authenticator tied to a user's biometric information, which makes it harder (but still not impossible) for them to trick the system

into giving them access. Depending on what biometric data is compromised — fingerprint, palm, voice, facial, iris or retinal data — it can be quite difficult, cumbersome or even impossible to take remedial actions (Hu & Zhang, 2016).

- **Limited recovery options:** While the FIDO2 authentication standard does allow the use of multiple authenticators, be it for backup purposes or to provide users with more choices, it does not permit the transfer of cryptographic user credentials between devices. Moreover, the standard does not provide any specific guidelines for the retrieval or revocation of authenticators that have been lost, damaged, or stolen (Kunke et al., 2021).

In all cases, it is essential to exercise caution when selecting an account recovery option because opting for an insecure method such as relying on backup passwords, sending OTP codes via SMS, or using insecure emails for receiving reset/recovery links can jeopardise the overall security of a system that otherwise complies with the FIDO2 standard (Alqubaisi et al., 2020).

At the time of writing, there is still an absence of a fallback authentication system or a robust account recovery mechanism within the FIDO2 standard. This means it is up to individual developers to incorporate their own mechanism to recover a lost account or authenticate users using an alternate method (Brendel, Clermont, & Fischlin, 2023; Kunke et al., 2021).

- **No syncing of credentials or keys between authenticators:** FIDO2 does not natively support credential or key syncing across multiple authenticators as its design philosophy is rooted in the idea of user-centric security, where the user's credentials are not stored centrally, thereby mitigating the impact of large-scale data breaches (Kepkowski,

Machulak, Wood, & Kaafar, 2023). This means that even if users have multiple authenticators, each authenticator has its own unique key pair, and there is no central authority that syncs or manages these keys across multiple devices for a single user. Therefore, each authenticator must be registered separately by the user.

However, it is worth noting that certain third-party password managers or identity providers may offer mechanisms to securely synchronise credentials across multiple devices, but these would be external to the FIDO2 standard and protocol itself. These solutions typically use a cloud-based service to store the credentials or keys, which are then communicated between authenticators using the FIDO2 protocol (Georgiadis, 2023). However, such solutions are typically vendor-locked as they are not part of the FIDO2 standard.

While the security, privacy, end-user experience, and usability of FIDO2 have received attention in academic literature in recent years, the difficulties associated with its integration and scalability within production environments still leave a lot to be desired. However, it is still a very promising new user authentication technology that offers a number of proven benefits over traditional password-based authentication methods.

The widespread adoption of FIDO2 depends on addressing the barriers of awareness, device compatibility, education, and cost. Collaborative efforts between technology providers, businesses, and user communities can help overcome these challenges and pave the way for a more secure online authentication landscape.

This section of the thesis aimed to draw attention to the FIDO2 authentication standard's strengths, limitations, and barriers to its widespread adoption. Although the standard itself is relatively new, the idea of passwordless authentication schemes certainly is not. As FIDO2 is still actively under development and full support from the members of the FIDO Alliance, every

incremental progress is laying down a solid foundation for bringing passwordless authentication to the mainstream at a slow but steady pace. With continued development and a growing user adoption rate, FIDO2 has the potential to become the standard for secure authentication in the near future.

2.2.2 Improved Security and Usability with aRBA

As the name would imply, Adaptive Risk-Based Authentication (aRBA) is a dynamic authentication process that assesses the risk level of each login attempt and adapts its authentication requirements accordingly. Instead of applying a one-size-fits-all approach, aRBA employs a multifaceted approach to determine the legitimacy or trustworthiness of a user's login request based on a number of criteria. By continuously assessing the risks associated with user login attempts, it offers a dynamic and flexible approach to authentication, which results in enhanced security whilst ensuring user convenience (Wiefling, Dürmuth, & Iacono, 2021, 2020).

2.2.2.1 Inner workings of aRBA

aRBA leverages contextual information and risk scoring to protect online accounts and services from fraudulent login attempts by dynamically adjusting authentication requirements based on the perceived level of risk associated with a particular login attempt (Ghorbani Lyastani et al., 2020).

It does so by taking various contextual, behavioural, and environmental factors into account for assessing the level of risk associated with any given login request. By doing so, aRBA strikes a good balance between security and user experience by offering a seamless yet secure authentication process. Figure 2.6 provides a simplified illustration of how aRBA works.

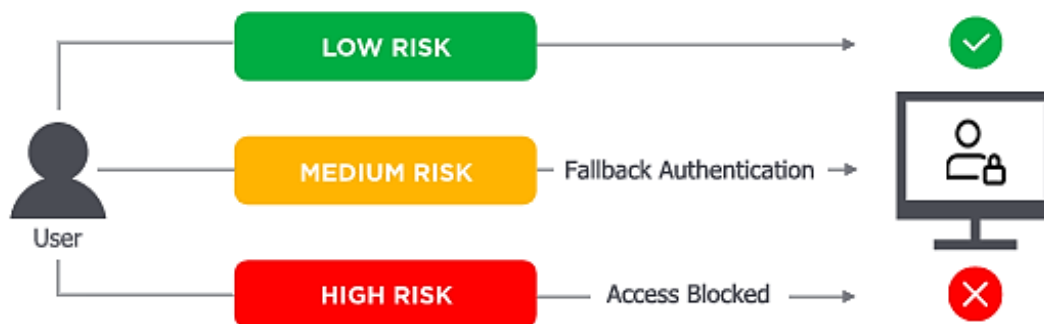


Figure 2.6: Implementation of an aRBA scheme dynamically responding to three different risk levels that indicate the likelihood of a fraudulent sign-in attempt and dynamically adapting the system’s authentication requirements as deemed appropriate.

2.2.2.2 Overview of the factors typically used by aRBA

As mentioned previously, the factors that aRBA uses to ascertain the legitimacy of a login attempt can broadly be categorised into three categories — contextual, behavioural, and environmental (Wiefling, Dürmuth, & Iacono, 2020).

Below is a non-exhaustive list of contextual factors:

- **Geolocation:** The user’s geolocation can be used to determine if the login attempt is coming from a known or unusual location. The user’s location may be captured and saved during registration.
- **IP address:** The user’s public IP address can be used to determine if the login attempt is coming from a range of known or unusual (suspicious) IP addresses. Wildcard masks are typically used to recognise users with dynamic IP addresses.

Detected IP addresses can also be automatically compared against an ever-growing database of all public IPv4 and IPv6 addresses with their reputation scores and other useful information. Suspicious or known malicious IP addresses trigger heightened authentication measures (Wiefling, Patil, Dürmuth, & Lo Iacono, 2020).

- **Time of day:** Similarly, the time of day can also be used to determine the risk of a login attempt. For instance, if a user typically logs in during normal business hours, but then suddenly a login attempt is detected during off-hours, then this may also be flagged as a medium to high-risk login attempt.
- **Device characteristics:** A user's device can also be used to determine the risk of a non-legitimate login attempt. For example, if someone typically logs in from a specific laptop or smartphone on a regular basis, but suddenly a new attempt is detected from an unfamiliar device, then this may be flagged as a high-risk login attempt.

There are several ways to uniquely identify devices, namely by using User-Agent strings, cookies, local storage, (device and browser) fingerprinting, client certificates, and MAC addresses for devices in a local network (Alappat, 2023).

- **Fingerprinting:** This technique combines a variety of attributes like screen resolution, canvas fingerprinting, operating system, User-Agent string, browser's name and version, installed browser extensions or plugins, time zone, locale, installed fonts, CPU architecture, battery status, form factor, and more to generate a unique fingerprint for each device belonging to a specific user. While it is not always exact, it can often be quite precise (Wiefling, Lo Iacono, & Dürmuth, 2019).
- **Historical data:** Historical data of previous login attempts and their outcomes can be used to build risk profiles and identify patterns of suspicious behaviour. Any deviation such as unusual login times, locations, or access patterns can trigger a higher-risk score, prompting the system to request additional authentication measures.
- **Network and traffic analysis:** Analysing network traffic patterns can help identify anomalies that may indicate an attack or an attempt to-

wards unauthorised access. Unusual network behaviour such as a sudden increase in data transfer or an unexpected surge in login attempts can trigger alarms. These anomalies can be factored into the risk assessment, prompting the system to take appropriate action like blocking access or stepping up authentication (Rivera et al., 2020).

Moreover, advanced machine learning algorithms can also be employed to analyse network and traffic data in real-time to identify patterns and trends associated with risky behaviour. These algorithms can continuously learn and adapt to make the system more accurate and effective over time.

Next are behavioural factors:

- **Behavioural biometrics:** A user's typical behaviour such as their typing speed, keystroke patterns, swipe patterns and gestures on touchscreens, and mouse movements can be monitored and analysed over time to build a behavioural profile for each user. Deviations from the norm may trigger additional authentication steps (Solano et al., 2021).
- **User behaviour analysis:** This involves analysing how a user normally interacts with a system or application by studying the patterns of their activities, preferences, and actions such as the pages they visit, the features they use, their location, the devices they use, frequency of their logins, and their historical usage data.

The user's past login behaviour information is used to determine if the current login attempt is unusual. For example, if a user typically logs in from the same location and device at the same time each day, and suddenly a login attempt is detected from a different location and device at an unusual time, then this may be flagged as a high-risk login attempt (Solano et al., 2021).

- **Machine Learning and AI:** Machine learning algorithms can be employed and trained using the behavioural data collected about each user to take a specific action if any anomalous or deviant behaviour is detected. Moreover, integration with third-party threat intelligence services would allow access to real-time data on emerging threats and known malicious actors.
- **User challenge and response:** Users may be challenged with questions or actions only they would know such as answering a security question, entering a one-time password or a biometric scan to determine if the user matches their claimed identity, thereby adding an extra layer of verification (Al Kabir & Elmedany, 2022; Kushwaha, Sonkar, Altaf, & Maity, 2021).
- **User's role and privileges:** Attempts to access sensitive data or perform actions outside of the user's typical role may be flagged as suspicious activity and an apt measure may be taken as a response.
- **Number of login attempts:** The number of login attempts made by the user can also be used as a behavioural factor. If a user makes multiple unsuccessful login attempts, this may be flagged as a suspicious, possibly automated, login attempt (Wiefling et al., 2019).
- **Login speed:** Tracking the speed at which a user enters their credentials is also used as a factor. If they enter their credentials abnormally quickly or slowly, this may be flagged as a suspicious login attempt.

Environmental factors include the user's physical environment such as the type of device they are using and the network they are connected to. This means that there can be some overlap between environmental and contextual factors in aRBA schemes as both of them contribute to the overall context of a login attempt and the level of risk associated with it.

This holistic approach allows for a more accurate evaluation of whether

a login attempt is likely to be legitimate or potentially fraudulent by considering all relevant information about it. The environmental factors used by aRBA schemes are as follows:

- **Session and device history:** Examining a user's recent session history and device usage can help detect anomalies or suspicious activities. Device and browser fingerprinting coupled with geolocation data play a crucial role in determining the overall environment from which a login attempt is being made (Koved, 2015). It would allow questions like the ones listed below to be answered.
 - Is the user attempting to log in from a known and trusted device or a new, potentially risky one?
 - Has the user's device or browser been compromised or manipulated in any way?
 - Is the combination of device and browser characteristics consistent with the user's historical behaviour, or does it raise any suspicion?
 - Is the user attempting to log in from their usual location?
 - Is the device being used geographically located in the regular location as the user?
- **Network anomalies:** Monitoring for network anomalies such as unexpected spikes in traffic, unusual network patterns, or suspiciously slow and unstable connection speeds can help detect potential security threats. A novel network latency profiling was proposed by (Rivera et al., 2020) to measure the risk score based on the network latency for 86 real users located across the globe. Their proposed profiling can detect 88.3% of attacks with an accuracy of 91.1% in distinguishing legitimate users from attackers.

- **Network connection type:** Network characteristics such as the user's connection type (cellular, WiFi, or wired connection), the use of VPN or proxy servers, and whether the user is attempting to access a system from a known corporate network or an unfamiliar location, etc. can all be used to form an educated guess of the login environment.
- **Geo-velocity:** While geolocation checks are performed to determine if the user is attempting to log in from an unusual or unfamiliar location, geo-velocity is measured to determine how quickly and realistically the user could have physically travelled to said location from their last verified location of a successful login attempt or session (Wiefling et al., 2019).
- **Proximity of known devices:** The proximity of other known devices associated with the user can also be considered. For example, if a user's smartphone is typically in close proximity to their laptop during logins, then a sudden attempt to log in without the same smartphone nearby might raise some suspicion (Papaioannou et al., 2021).
- Other contextual factors such as the number of login attempts and frequency, device type, time of day, network connection, physical location of the device being used, and security posture of the device are also often used to work out the overall environment from which a login attempt is being made.

2.2.2.3 How risk scores are calculated

The heart of aRBA lies in the calculation of risk scores for each login attempt. It is a numerical value that represents the perceived riskiness of any given login attempt. These scores are determined by assigning weights to various risk factors based on their importance in assessing the risk of a fraudulent login attempt (Wiefling, Dürmuth, & Lo Iacono, 2021). For instance, device

profiling or fingerprinting would generally carry more weight than geolocation (Papaioannou et al., 2023).

As each factor is assigned a weight based on its significance in determining the risk level, various algorithms are used to calculate the risk score by analysing these factors collectively. This score is then compared to a pre-defined threshold as it quantifies the level of risk associated with a given login attempt. Depending on the score's magnitude, the system then dynamically decides in real-time if stricter authentication methods will have to be applied or if the attempt should be blocked altogether in the event of a high enough risk score (Wiefling, Jørgensen, Thunem, & Iacono, 2022).

The figure below illustrates how aRBA effectively decides which route to take whenever a new login attempt is made by a user.

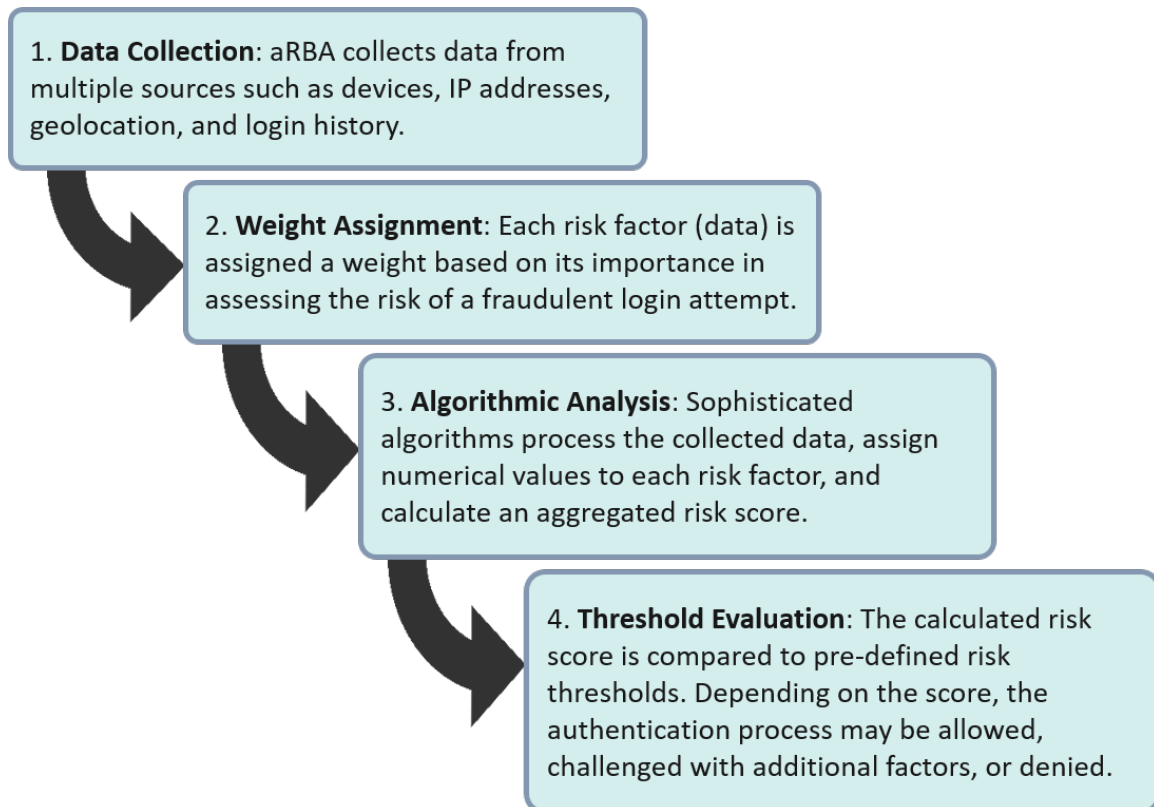


Figure 2.7: Flowchart of how various factors are weighted in aRBA schemes to determine the risk of a fraudulent login attempt by calculating an aggregated risk score.

Based on the risk score, aRBA schemes trigger predefined adaptive policies. These policies dictate the appropriate authentication mechanisms for each risk level, ranging from allowing access to the user without any further hindrance to posing additional challenges to the user to verify their identity or even denying them access straightaway.

2.2.2.4 Categorisation of risks

As mentioned previously, the calculated risk scores are compared against a predefined threshold to categorise them into low, medium, and high-risk levels of risk. Each level corresponds to a fallback authentication (or lack thereof) as it is up to the organisations to define risk thresholds and policies that determine what actions may be taken based on the calculated risk score.

Generally speaking, a higher score typically indicates a higher chance of a fraudulent login attempt and it will be dealt with accordingly. This allows aRBA schemes to offer a better balance of usability and security than any other static user authentication system to date (Wiefling et al., 2022).

A breakdown of what actions a typical aRBA scheme may take is given below (Wiefling, Dürmuth, & Iacono, 2021).

- Low-risk login attempts may be granted access with minimal or no additional authentication challenge.
- Medium-risk attempts might trigger multi-factor authentication (MFA) like a one-time password (OTP) sent to a registered email address or smartphone or step-up authentication by imposing additional security measures like biometric authentication.
- High-risk events might trigger access denial or temporary account lockout with an alert being sent to the user's registered email address or phone number.

2.2.2.5 Benefits of implementing aRBA

It can be argued that the way aRBA dynamically handles user authentication is essential in today's digital landscape, where newer, more sophisticated cyber threats are constantly emerging, and traditional static authentication methods are no longer deemed sufficient to protect users' data and resources. Some of the other notable benefits of implementing aRBA are listed below (Wiefling, Dürmuth, & Iacono, 2020).

- **Enhanced security:** aRBA schemes provide a dynamic form of defence against a wide range of threats, adapting to changing attack patterns and responding to anomalies in real-time to reduce the likelihood of unauthorised access. Based on the calculated risk score, aRBA schemes trigger predefined adaptive policies. These policies dictate the appropriate authentication mechanisms for each risk level. It therefore helps reduce fraud and account takeovers by identifying and blocking fraudulent login attempts (Wiefling, Patil, et al., 2020).
- **Enhanced user experience:** aRBA balances security with user convenience by only requesting additional authentication when necessary, reducing friction during routine login attempts. This allows systems with aRBA schemes to provide a better user experience by minimising unnecessary authentication steps during low-risk situations, resulting in quicker and more convenient logins (Al Kabir & Elmedany, 2022).
- **Customisability:** Organisations can tailor aRBA schemes to their specific needs, adjusting risk thresholds and authentication requirements to align with their risk tolerance levels and userbase's preferences.
- **Dynamic adaptability:** aRBA schemes maintain user profiles that accumulate historical data about each user's behaviour and authentication patterns. This profile evolves over time as the user interacts with a given system. Analysing historical data provides valuable context

for the scheme to make informed decisions about risk levels and authentication requirements during each login attempt.

- **Real-time analysis and adaptation:** aRBA operates in near real-time, analysing data as it is collected to provide an immediate response to each authentication attempt. This ensures a seamless user experience while maintaining a high level of security. These schemes dynamically adjust authentication requirements based on the perceived risk of each login attempt as illustrated in the figure below.

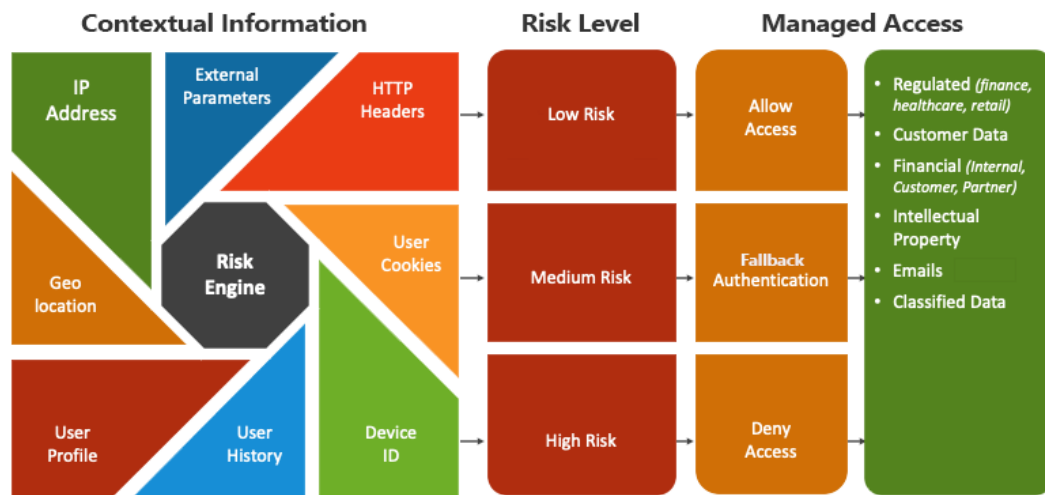


Figure 2.8: High-level overview of a typical aRBA system in action.

As a user's behaviour and risk profile can change over time, the scheme continuously reassesses the risk and adjusts the authentication requirements accordingly (Yamaguchi, Nakata, & Kobayashi, 2020). For example, if a previously low-risk user starts exhibiting unusual behaviour, the system may elevate their risk score and prompt for additional authentication to ensure that it is the same person.

- **Continuous improvement:** aRBA schemes are designed for continuous improvement. As new attack vectors emerge and user behaviours evolve over time, sophisticated machine learning algorithms adapt to

these changes for ensuring that the authentication scheme remains effective at mitigating risks of account takeovers from occurring. This makes such schemes a resilient form of defence against emerging attack vectors.

2.2.2.6 Limitations of aRBA and its barriers to widespread adoption

Although aRBA is a promising approach to enhance security and convenience of users, it also comes with its share of limitations and adoption hurdles. One significant limitation is the reliance on accurate risk assessment, which can be challenging to achieve as it entails monitoring users' behaviours continually and taking multiple factors into consideration for establishing a baseline risk score for each user. Most of its other limitations and barriers to widespread adoption are as follows.

- **Privacy concerns:** The amount of data that is typically collected and analysed to build as well as maintain user profiles and their behavioural information often tend to raise privacy concerns. Organisations must therefore comply with governing privacy regulations by collecting only what is strictly necessary and implement stringent data protection measures to safeguard all stored user information in addition to having the ability to opt out of using aRBA schemes with the option to permanently delete any stored data tied to the user's likeness (Wiefling, Tolsdorf, & Iacono, 2021).
- **False positive detection:** Overly aggressive risk assessment may result in false positives, thereby inconveniencing legitimate users by flagging their login attempts as high risk and potentially causing frustration by triggering authentication challenges too frequently.
- **False negative detection:** Conversely, if an aRBA scheme fails to detect an actual risk by undermining a risk factor and giving it a lower

score, then this could potentially allow malicious actors to gain access to a system and perform fraudulent transactions. This is a significant concern because it means that the system is not providing the intended level of security (Solano et al., 2021).

- **Other accuracy concerns:** Accurate risk assessment depends on precise user behaviour modelling, which can be challenging due to evolving user habits and the potential for inaccuracies. Moreover, as the effectiveness of aRBA schemes rely heavily on the availability and accuracy of contextual data, incomplete or inaccurate information can likely affect risk assessments. This means cybercriminals may be able to manipulate contextual factors to appear as low-risk users, thereby bypassing the stronger authentication measures of a system.
- **User resistance:** Users' perception of aRBA schemes as invasive or cumbersome may cause them to be uncomfortable with the idea of their behaviours being continuously monitored for authentication purposes and the potential for increased friction or delay in the authentication process due to false positive detection (Wiefling, Dürmuth, & Iacono, 2020).
- **Implementation complexity:** Deploying aRBA schemes often require significant technical expertise and resources as it requires a deep understanding of user behaviour, risk factors, and advanced data analytics. This added complexity can make it less accessible to smaller organisations. Moreover, there is also a need for standardised risk assessment methods and frameworks to allow for widespread adoption.
- **Integration challenges:** Integrating aRBA into existing authentication systems can be challenging, especially in complex IT environments with large, existing legacy systems and a vast number of daily active users where prolonged system downtime is not ideal. It may

also require integration with various systems and the development of customised risk-scoring algorithms depending on organisations' needs (Unsel, Wieffling, Gruschka, & Lo Iacono, 2023).

- **Constant maintenance and updates:** aRBA schemes need to be continuously maintained and updated to remain effective as threat landscapes evolve over time. Machine learning risk-scoring models must constantly be trained and tuned for adapting to new threats and vulnerabilities (Liu, Liu, & Lai, 2022).
- **Higher overall costs:** Implementing aRBA can involve significant upfront costs for the procurement or development of risk-scoring models and training the AI models to continuously analyse user behaviours to be able to accurately surmise if future attempts are being made by the same person or not. Furthermore, the maintenance and operating costs of aRBA systems can be resource-intensive given how much data of each and every user needs to be collected to monitor as well as analyse their behaviour and other factors for login patterns and threats.

2.3 Discussion: Why combine the two?

As of the time of writing, the idea of incorporating FIDO2 into an adaptive risk-based authentication scheme is not entirely a novel concept as it was already being discussed and explored independently by security experts and organisations. However, there is still a sizable research gap in the world of academia, especially when it comes to its feasibility in the real world. Therefore, it is an evolving trend in the field of cybersecurity as this approach combines the strength of FIDO2's passwordless authentication with adaptive risk assessment to provide enhanced security while ensuring a seamless user experience. The idea is to adapt the authentication process based on the perceived risk associated with a specific user or transaction. This combination

can therefore provide a good balance between security and user convenience. Strong authentication with biometrics or hardware tokens can be used when the risk is high, and less intrusive methods may be employed when the risk is lower.

The proposed multi-factor scheme would use FIDO2 to create and store strong authentication credentials locally and only share the bare minimum amount of encrypted information to authenticate or re-authenticate a user online by utilising aRBA to automatically determine the level of authentication required for each login attempt using risk scores calculated by analysing certain preset factors. This would allow a multi-factor user authentication scheme such as the proposed scheme to achieve a high level of security while also minimising user inconveniences and putting most privacy concerns to rest by collecting information that is strictly necessary and obfuscating any sensitive information before its transmission or storage.

Thus, this thesis theorises that FIDO2 and aRBA are two complementary technologies which can be used in tandem to build on — or benefit — from each other's strengths and also address or overcome the limitations of each other. FIDO2's strong and secure authentication methods and aRBA's adaptability in responding to evolving risks and different login circumstances would make their combination a powerful defence against most cyber threats. Moreover, as discussed previously, aRBA's risk analysis capabilities ensure that the appropriate level of authentication is applied at any given moment, reducing friction for low-risk login attempts and fortifying protection for high-risk attempts. The result is a comprehensive authentication solution that not only offers robust security, but also ensures a seamless and user-friendly experience with user privacy in mind.

Chapter 3

Methodology

3.1 Overview

This chapter lays the groundwork for exploring the feasibility of a novel multi-factor user authentication scheme that combines both FIDO2 and aRBA technologies. The proposed scheme, aptly titled “Adaptive Risk-based Passwordless Authentication” or ARPA for short, would leverage FIDO2 to provide a strong foundation for user authentication in lieu of passwords, and then use aRBA to dynamically adjust the level of authentication or re-authentication required based on the calculated risk level of any given login attempt. It is believed that this scheme could provide a significant improvement in user authentication security, while also maintaining a high level of user convenience (usability) and privacy.

Thus, a study was conducted that can broadly be split into two phases — the development of a basic, working proof-of-concept and the assessment of its practicality, efficiency, and user acceptance.

Moreover, the adopted research methodology was also comprised of data collection, analysis, and interpretation, which was crucial for achieving a holistic understanding of the proposed user authentication scheme's feasibility.

3.2 Research Design

The research design of this thesis is experimental as it involves the creation and testing of a basic, working proof-of-concept authentication scheme. This design was chosen since it allows for controlled testing and evaluation of the proposed user authentication scheme's effectiveness as a viable candidate for doing away with passwords and user acceptance. The experimental design rationale may be summarised as follows:

- **Controlled environment:** Conducting an experiment enables the creation and testing of a basic, working proof-of-concept of the proposed ARPA scheme within a controlled setting. This allows for systematic manipulation of relevant variables and isolation of specific factors that influence the scheme's overall performance and effectiveness. Therefore, experimenting allows for several crucial questions to be answered in a satisfactory manner with the necessary data to quantify the impact of the proposed scheme.
- **Effectiveness evaluation:** The experiment facilitates measuring the effectiveness of ARPA in terms of security, usability, and user acceptance. Metrics such as login success rates, authentication times, error rates, and user feedback data through surveys can be collected and analysed to assess the scheme's viability as a potential multi-factor passwordless solution.

- **User acceptance considerations:** User acceptance is crucial for any system's success. The experimental design includes surveying participants after testing the ARPA scheme prototype to gather their subjective experiences and preferences, thereby providing valuable insights for further refinement in future revisions of the proposed scheme and potential real-world adoption.

However, due to constraints imposed by time and resources, the following additional considerations had to be deferred for future studies that will build on the strong foundation laid by this thesis.

- **Survey design:** The close-ended nature of the survey questions limit the depth of information available for analysis and primarily results in quantitative data being gathered, which often have to be complemented with qualitative data for drawing better conclusions. Therefore, open-ended questions could prove to be beneficial for capturing more nuanced feedback from users.
- **Iterative development:** By adopting an iterative development of the ARPA scheme and its subsequent user testing, the results obtained would allow the scheme to be refined over time, thereby improving its odds of real-world adoption.

Overall, the chosen experimental design provides a robust framework for evaluating the feasibility and potential of the proposed user authentication scheme. It allows for controlled testing, objective data collection, and collecting valuable insights into user acceptance, thus paving the way for future development and potential real-world implementation.

3.3 Data Collection Methods

Data collection methods for this endeavour was comprised of the development of a basic prototype, user testing, filling a survey questionnaire, and taking ethical questions into consideration.

3.3.1 Prototype Development

A basic, working proof-of-concept of the proposed authentication scheme (ARPA) that combines FIDO2 and aRBA was developed as a prototype, and this then served as the foundation for testing and evaluation. This acted as the primary data collection instrument for capturing user interactions, authentication attempts, and system responses for further analysis.

3.3.1.1 Technology Stack

The ARPA prototype and its accompanying dummy web application were written in PHP and JavaScript due to their speed and simplicity. The entire project was hosted on 000webhost's free hosting plan and backed up in Google Drive for seamless file storage and access online.

- **FIDO2 Integration:** The open source FIDO2 standard, which encompasses WebAuthn 2 API and the CTAP 2.1 protocol, is integrated into ARPA in a way that ensures compliance with industry standards to maximise cross-platform compatibility.

The standard was implemented with the help of server resources that were shared on GitHub by web-auth ¹, fido2-lib ², lbuchs ³, and lyokato ⁴ for allowing the dummy web application (RP) to commu-

¹ <https://github.com/web-auth/webauthn-framework>

² <https://github.com/webauthn-open-source/fido2-lib>

³ <https://github.com/lbuchs/WebAuthn>

⁴ <https://github.com/lyokato/WebAuthnKit-Android> | [WebAuthnKit-iOS](#)

nicate with the FIDO server. Furthermore, server-side libraries and numerous other resources by Spomky-Labs ⁵, madwizard.org ⁶, LINE Engineering ⁷, herrjemand ⁸, deepzz0 ⁹, and MasterKale ¹⁰ were also found to be immensely helpful during the back-end implementation of this project.

As the FIDO2 standard is supported by nearly all major web browsers and operating systems, there are no prerequisite client-side libraries required, so JavaScript methods like `navigator.credentials.create()` and `navigator.credentials.get()` can directly be invoked for interacting with FIDO2-compliant authenticators whenever required.

- **Adaptive Risk Engine:** The ARPA scheme was complemented with a converted and modified version of the open source aRBA implementation ¹¹ put forward by (Wiefling et al., 2022) and (Unsel et al., 2023), which in turn is based on an algorithm and statistical framework for identifying suspicious login attempts that was originally developed and published by (Freeman, Jain, Dürmuth, Biggio, & Giacinto, 2016), but with several tweaks and other improvements to further optimise its performance and accuracy.

This adaptive risk analysis engine was incorporated into the proposed authentication scheme for continuously monitoring user behaviour as well as other factors or attributes such as device type, IP address, geolocation, and geo-velocity, and then adjusting authentication requirements dynamically as deemed appropriate.

⁵ <https://github.com/Spomky-Labs/otphp>

⁶ <https://github.com/madwizard-org/webauthn-server>

⁷ <https://github.com/line/line-fido2-server>

⁸ <https://github.com/herrjemand/awesome-webauthn>

⁹ <https://github.com/deepzz0/awesome-fido2>

¹⁰ <https://github.com/MasterKale/SimpleWebAuthn>

¹¹ <https://github.com/das-group/rba-algorithm/blob/main/rba-algorithm.ipynb>

3.3.1.2 Technical Diagrams

This subsection delves into the intricate workings of the ARPA scheme through a series of technical diagrams to provide some much-needed insights in a concise yet comprehensive manner.

Figures 3.1 and 3.2 illustrate a high-level overview of the registration and login flows of the ARPA scheme by showcasing the seamless interaction FIDO2 passwordless authentication and an adaptive risk analysis engine that continually checks for any abnormalities which can lead to a higher risk score and subsequent measures being taken to prevent an account takeover from occurring.

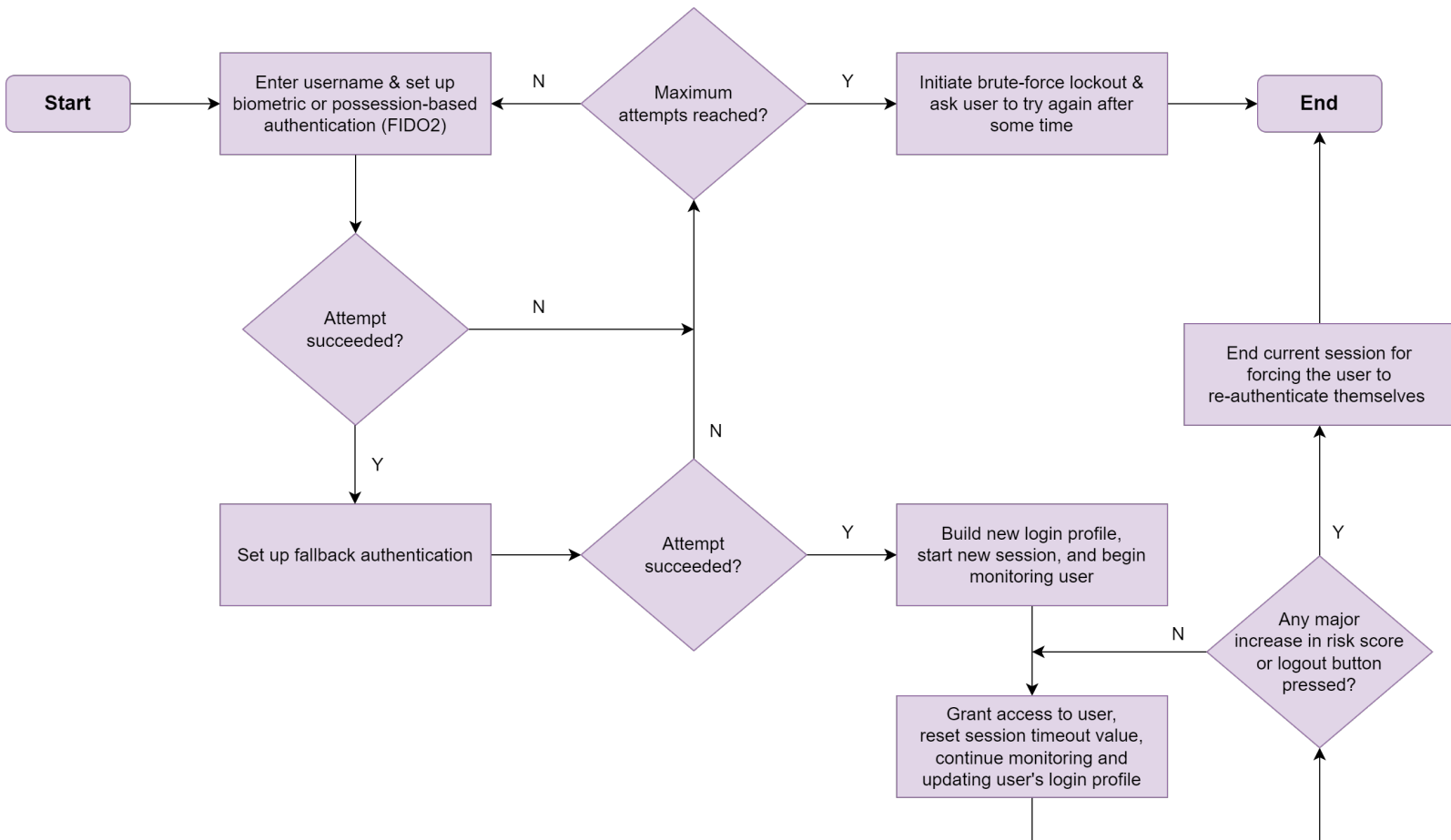


Figure 3.1: Simplified flowchart of the user registration flow in the proposed ARPA scheme.

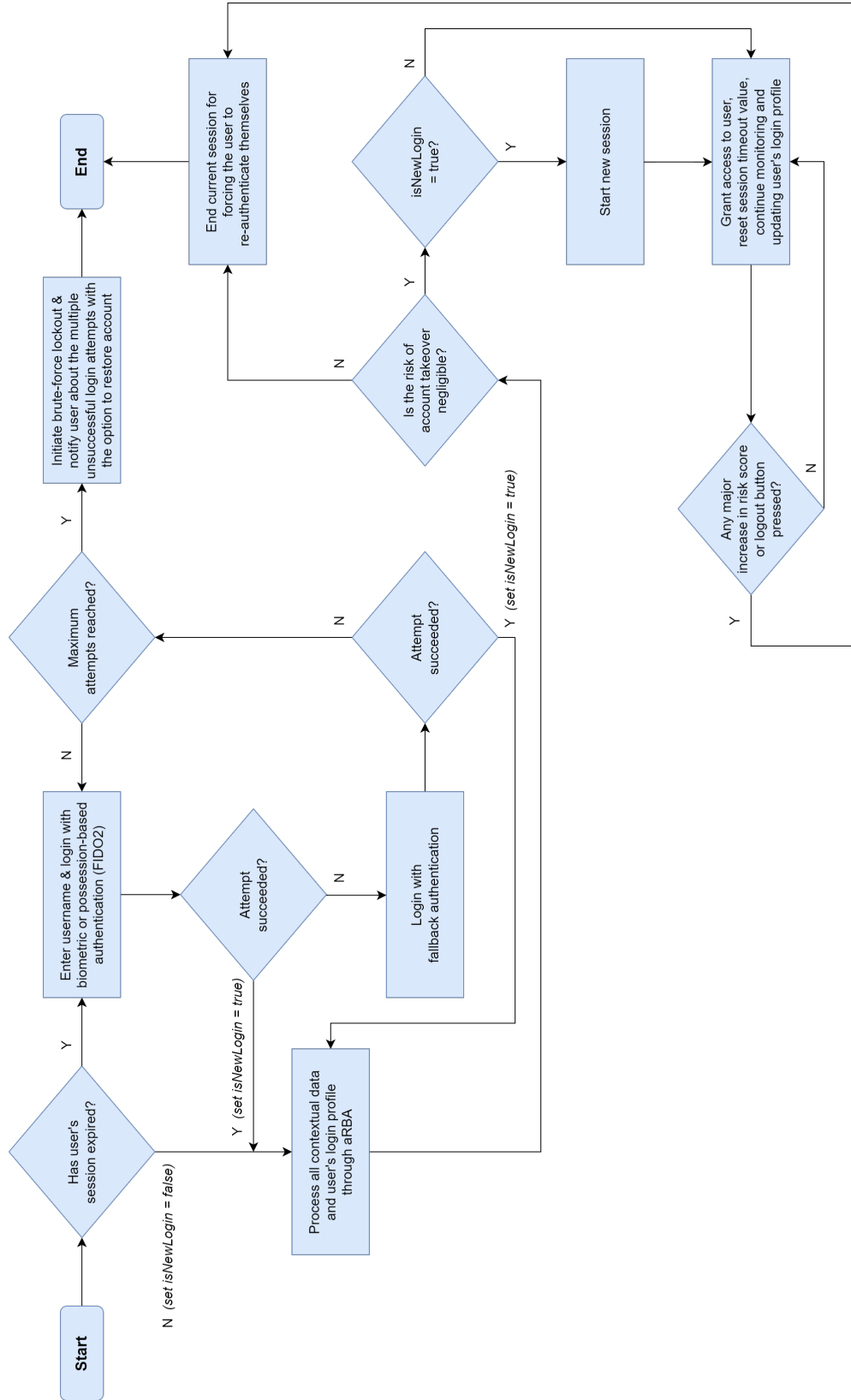


Figure 3.2: Simplified flowchart of the user login flow in the proposed ARPA scheme.

These flowchart diagrams depict the registration and login flows of the ARPA scheme by drawing attention to how it uses FIDO2 for allowing users to use biometric as well as possession-based authentication and aRBA to automatically grant access to a user if it deems that the same person is indeed trying to access the system by taking several contextual factors and environmental parameters into account for positively identifying the intended user. Moreover, all the figures in this subsection serve as a valuable tool for readers by enabling them to grasp the technical underpinnings of the ARPA scheme and appreciate the intricate interplay between its core elements.

For instance, the next two figures, 3.3 and 3.4, illustrate how the ARPA scheme utilises the open source FIDO2 authentication standard to allow secure, convenient, and passwordless user authentication across all supported web applications and devices.

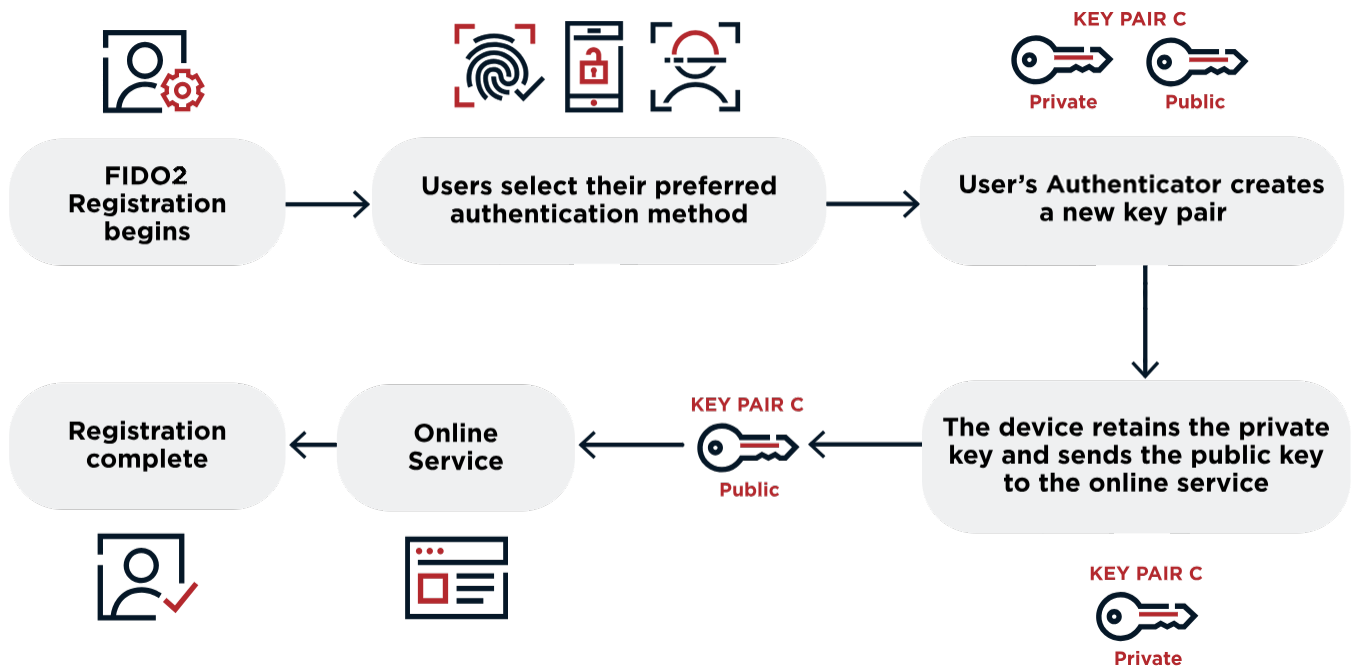


Figure 3.3: Simplified illustration of the user registration process powered by FIDO2 in the proposed ARPA scheme.

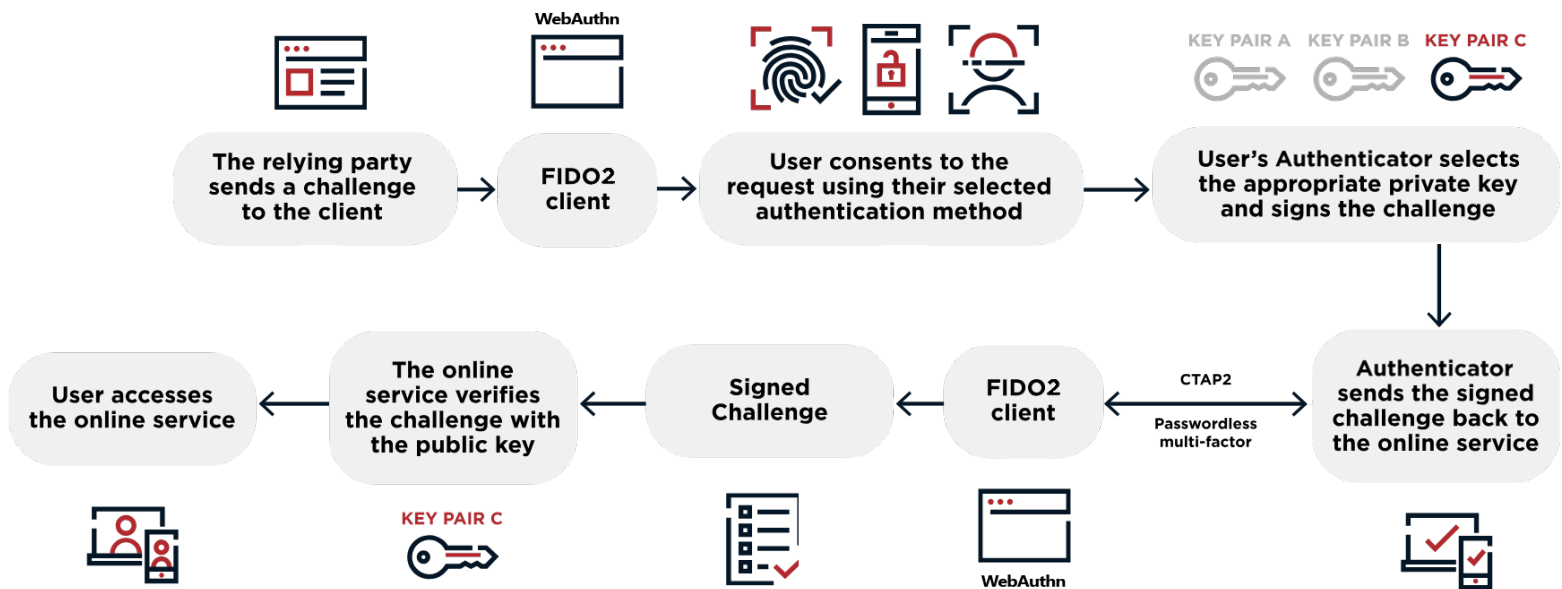


Figure 3.4: Simplified illustration of the passwordless user login flow powered by FIDO2 in the proposed ARPA scheme.

By presenting the technical complexities of the ARPA scheme through these simple visuals, this subsection attempts to pave the way for an easier and deeper understanding of the proposed user authentication scheme's potential to be a viable candidate for deprecating the use of passwords. It also serves as a good of reference for future research and developmental efforts.

Hence, subsequent figures illustrate how the proposed scheme's internal risk engine continually evaluates the level of risk associated with any given login attempt and the necessary courses of action it automatically takes based on the risk score calculated using contextual factors and other environmental parameters. If a non-negligible risk is detected, an authentication challenges is dynamically posed to the user, and the success or failure of this challenge determines the user's access being granted or blocked, thereby completing the loop as this is a continuous authentication process.

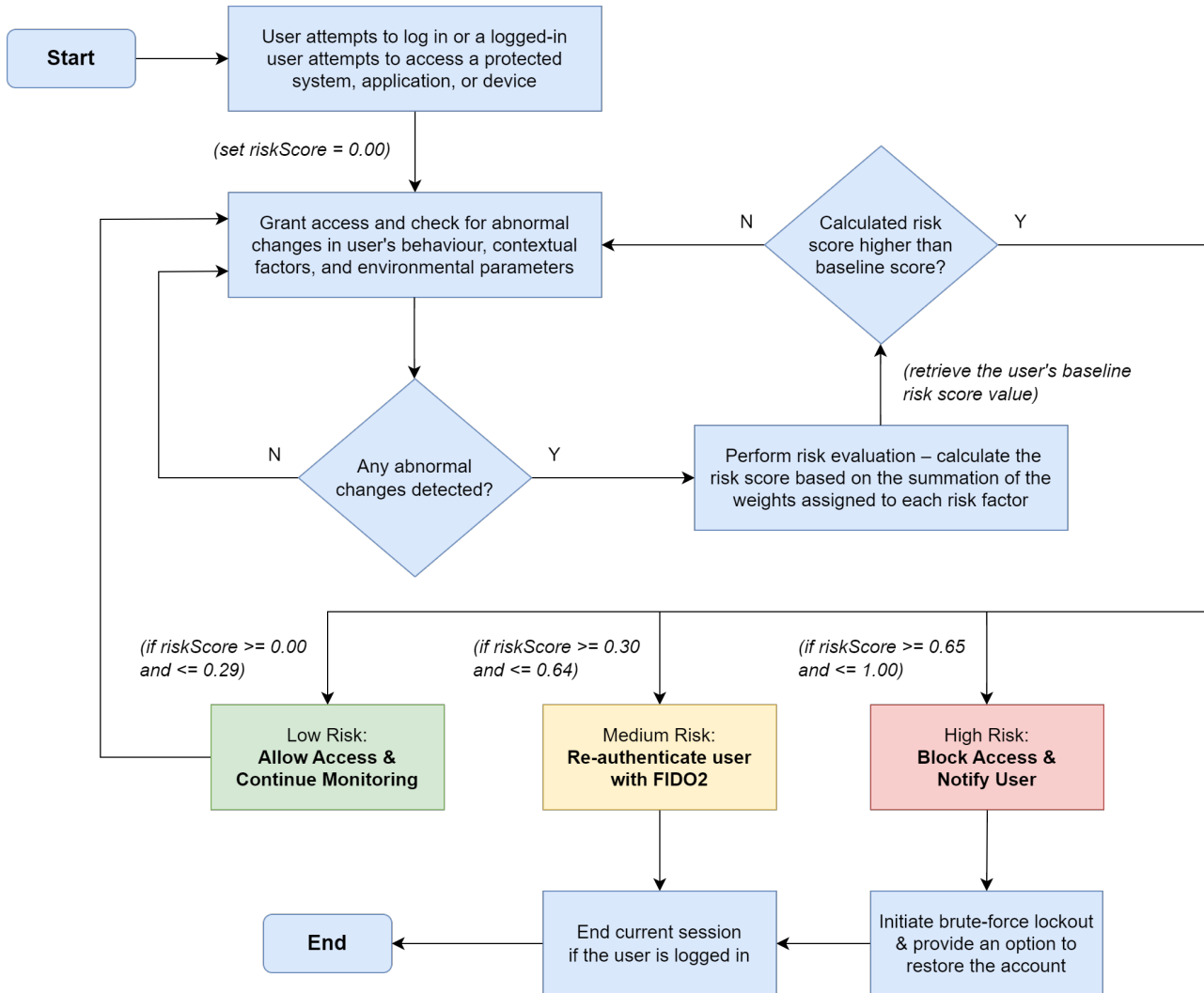


Figure 3.5: Simplified internal logic of the risk analysis engine component of the proposed user authentication scheme to dynamically safeguard user accounts.

As depicted in Figure 3.5 above, the risks of account takeover are categorised into low, medium, and high, which are determined by comparing each user's baseline risk score with the score calculated by combining the weights of each contributing factor. This baseline score is calculated from the users' login profile based on their trends and other information collected about them over a period of time since the initial registration.

aRBA effectively works by assigning risk scores to every login attempt

and resource access requests based on certain factors like IP addresses, geolocation, geo-velocity, device fingerprinting, and changes in users' behaviour as well as their login trends to name a few. The risk score range for the three categories of risk in the ARPA scheme's risk engine are as follows:

- **Low Risk** — *0.00 - 0.29*
- **Medium Risk** — *0.30 - 0.64*
- **High Risk** — *0.65 - 1.00*

This ranging of risk scores serves as a promising starting point for balancing users' security and convenience. However, the exact ranges will naturally differ from one system to another based on security requirements. These ranges and the assigned weights of each factor will likely have to be adjusted due to key aspects such as continuous monitoring, system's performance, resource requirements, userbase, user feedback, and evolving threat landscape for optimal effectiveness of the proposed ARPA scheme. Iteratively optimising a system based on collected historical data and user feedback will allow for a more robust, adaptive passwordless authentication scheme that effectively balances security and convenience for its end-users.

aRBA maximises user convenience by minimising user fatigue and frustration from frequent verification prompts, but at the same time, it might also create inconvenience for legitimate users experiencing temporary changes in their contextual, behavioural, and environmental data due to travelling, change of residency, or switching to a new device, for instance. Therefore, carefully setting and fine-tuning thresholds within the risk score range is crucial. Analysing user behaviour and feedback can reveal whether specific ranges or thresholds need adjustments — narrowed or widened — to optimise for increased security or smoother user experience respectively.

Moreover, establishing a dynamic baseline risk score for each user account proves to be a vital component in adaptive risk-based authentication

as it allows for reduced user friction due to improved accuracy over time, enhanced anomaly detection, customised risk thresholds, better profiling, and a personalised real-time risk assessment that is always up-to-date. It is also crucial to reassess risk scores periodically during active sessions and comparing it to the baseline risk score to detect potential anomalies in real-time even after initial authentication.

Table 3.1: Weighting of the most commonly used factors in the adaptive risk engine component of the proposed ARPA scheme.

Factor	Risk Rating	Weighting	Description
General User and Device Information			
User Identity Profile	High	0.25	Admin or high-value user accounts deserve higher weights.
Device	Medium	0.15	Unknown devices warrant more scrutiny than trusted ones.
Language Preference	Low	0.10	Sudden change in language preferences could warrant some scrutiny.
Operating System	Low	0.10	Outdated or uncommon versions might increase suspicion.
Browser Version	Low	0.05	Outdated or uncommon versions might increase suspicion slightly.
Browser Extensions	Medium	0.15	Presence of uncommon or potentially risky browser extensions and/or the sudden absence of a common one could slightly raise suspicion.
Location and Time-Based Factors			
IP Address	High	0.20	Unfamiliar or high-risk locations raise the score. Moreover, IP addresses from known malicious sources raise the risk significantly.
Geolocation	High	0.20	Unexpected locations might warrant additional scrutiny.
Geo-velocity	Medium	0.15	Uncharacteristically rapid location changes raise concerns.
VPN Usage	Medium	0.15	Connecting (or not connecting) from VPNs could raise suspicion depending on organisational security policies.
Time of Day	Low	0.10	Login attempts outside usual hours might deserve slight scrutiny.
Day of Week	Low	0.05	Weekends or holidays might see slightly different access patterns.
Behavioural and Session-Based Factors			
Login Attempts	Medium	0.15	Multiple failed attempts suggest potential compromise or hacking attempt.
Time to Authenticate	Low	0.10	Unusually long delays could indicate hesitation or difficulty.
Session Duration	Low	0.10	Abnormally short or long sessions might deserve a check.
Unusual Activity	High	0.25	Accessing sensitive data or resources from unfamiliar devices or locations.
Interaction Patterns	Medium	0.15	Unusual mouse movements, keyboard strokes, or scrolling/clicking patterns could indicate deviation from typical user behaviour.
Threat Intelligence and External Data			
Device Fingerprinting	Medium	0.15	Unknown devices warrant more scrutiny than trusted ones.
IP Reputation	Medium	0.15	Known malicious IP addresses trigger higher risk.
Network Anomalies	High	0.25	Sudden spikes in Time to First Byte (TTFB), Round-Trip Time (RTT), and overall latency is a cause for concern.
Previous Security Incidents	Medium	0.15	Accounts with compromised credentials and other details such as email addresses and phone numbers due to data breaches warrant extra attention.

Table 3.1 enumerates the weighting of the most commonly used factors in aRBA. A considerable change in the value of any of those listed factors will result in its weightage being added to the calculated risk score. This aggregated risk score is then compared with the baseline risk score to determine how much of a discrepancy exists between the two scores. Naturally, a higher discrepancy would indicate a higher risk of a fraudulent login attempt.

It may be noted that the basic, working prototype version of the ARPA scheme featured in this thesis paper does not include all of the factors commonly used to identify a user as it would have added further complexity and delays in the development of the prototype as well as its initial training and testing with volunteers to establish a baseline. As a result, only a select few risk factors were chosen to be included, trained, and then tested in the prototype version of the proposed passwordless multi-factor user authentication scheme as illustrated in the figure below.

	Device Fingerprint	IP Address Familiarity	Geolocation	Geo-velocity	Login Trend or History	Behavioural Biometrics	Network Anomalies	
User 1  Low Risk Attempt	 Using familiar or trusted device	 Using known or trusted IP address	 Familiar region or country	 Within acceptable range	 Within acceptable range	 Fits user's past login behaviour	 Within acceptable range	Allow access without further hindrance
User 2  Med. Risk Attempt	 Using unfamiliar device	 IP address in known range	 Login request somewhat nearby	 Within acceptable range	 Slight deviation observed	 Negligible change in behaviour	 Higher latency, TTFB, and RTT	Challenge with fallback FIDO2 authn.
User 3  High Risk Attempt	 Using unfamiliar device	 Unfamiliar or known "bad" IP address	 Unfamiliar region or country	 Physically beyond range	 Major deviation observed	 Anomalous behaviour observed	 Higher latency, TTFB, and RTT	Deny access and notify user

(^ risk factors used by the adaptive risk engine of the proposed ARPA scheme ^)

Figure 3.6: Factors used by the adaptive risk engine for scoring each login attempt to determine the identity of the intended user in the prototype version of the ARPA scheme.

From the very first login to logout, aRBA continually monitors various biometric, behavioural, and contextual data in real time to confirm and re-confirm a user's identity and flag anomalies as they are being detected. If the system detects a considerable change to pre-determined user patterns and the subsequent deviation from the baseline risk score, then the current session of the account in question is automatically ended, and the user is forced to re-authenticate themselves using FIDO2-based authentication to re-confirm their identity.

3.3.1.3 Risk Score Calculation Model

Equation 3.1 below is a slightly modified variant of the model put forward by (Freeman et al., 2016) and later extended by (Wiefling et al., 2022) to calculate the risk score S for the login attempt of a user u and a given feature value set $(FV^1, \dots, FV^d)$ with d features or factors such as the IP address, geolocation, device in use, browser type, operating system, etc.

$$S_u(FV) = \left(\prod_{k=1}^d p(attack|FV^k) \frac{p(FV^k)}{p(FV^k | u, legit)} \right) \frac{p(u | attack)}{p(u | legit)} \quad (3.1)$$

The calculation takes a few probabilities into account for generating a risk score, namely:

- The attack probability $p(attack|FV^k)$ denotes the number of feature value occurrences in failed login attempts, with the minimum probability set to

$$p(attack|FV^k) = \frac{1}{total\ number\ of\ attacks}$$

if the feature value is not present in the attack data as it is assumed that a residual risk of other feature values (factors) being used in an attack is always present.

- $p(FV^k)$ is the probability of a feature value existing in the global login history of all users.
- $p(FV^k | u, legit)$ is the probability of a feature value to appear in the legitimate user's login history as it is likely to be in use whilst the login attempt is being made.
- As $p(u | attack)$ estimates how likely a user is being attacked, and all users are assumed to be targeted at some point, it is set to $\frac{1}{U}$ where U is the set of all users with $u \in U$ and the minimum probability is set to

$$p(u | attack) = \frac{1}{total\ number\ of\ logins}$$

as it is based on the number of failed login attempts per user.

- And finally, $p(u | legit)$ is the probability of how likely the intended user is attempting to sign in, so it is derived from

$$(p(u | legit) = \frac{number\ of\ user\ logins}{number\ of\ all\ logins}$$

It may be noted that for some feature values such as IP addresses, the odds of an exact match can sometimes be low as the user's ISP might be providing a dynamic IP address or if their smartphone is on the move, which results in it switching between cell towers. This can result in $p(FV^k | u, legit)$ equalling to 0, which would incorrectly flag every login attempt as suspicious.

To compensate for frequently changing feature values, sub-features may be derived from the primary feature value to mitigate the effects of such cases. For instance, an IP address may be dissected and then analysed for information such as the name of the ISP, Autonomous System Number (ASN) and its range, and of course, the country or region the IP address belongs to. Moreover, the last octet of an IP address may also be discarded if it is deemed necessary to allow for more margin of error.

It is therefore evident that the calculation of risk scores greatly depends on the global login history size, so granularity of the scores increase as the number of entries in the global login history increases over time.

The attack data also plays a huge role in this statistical model due to its relatively simplistic yet effective nature. This model can surely be enhanced with the introduction of intelligent machine learning to greatly increase the accuracy of determining if it is the same person attempting to login from one attempt to the next and be able to learn and score each login attempt with greater precision, however this is currently beyond the scope of this thesis.

3.3.1.4 Database Schema

The database schema below outlines a simplified but robust framework for a modern aRBA engine complemented by FIDO2 technology, where usability and security are maximised whilst also attempting to deprecate the use of passwords for good as illustrated in Figure 3.7 below.

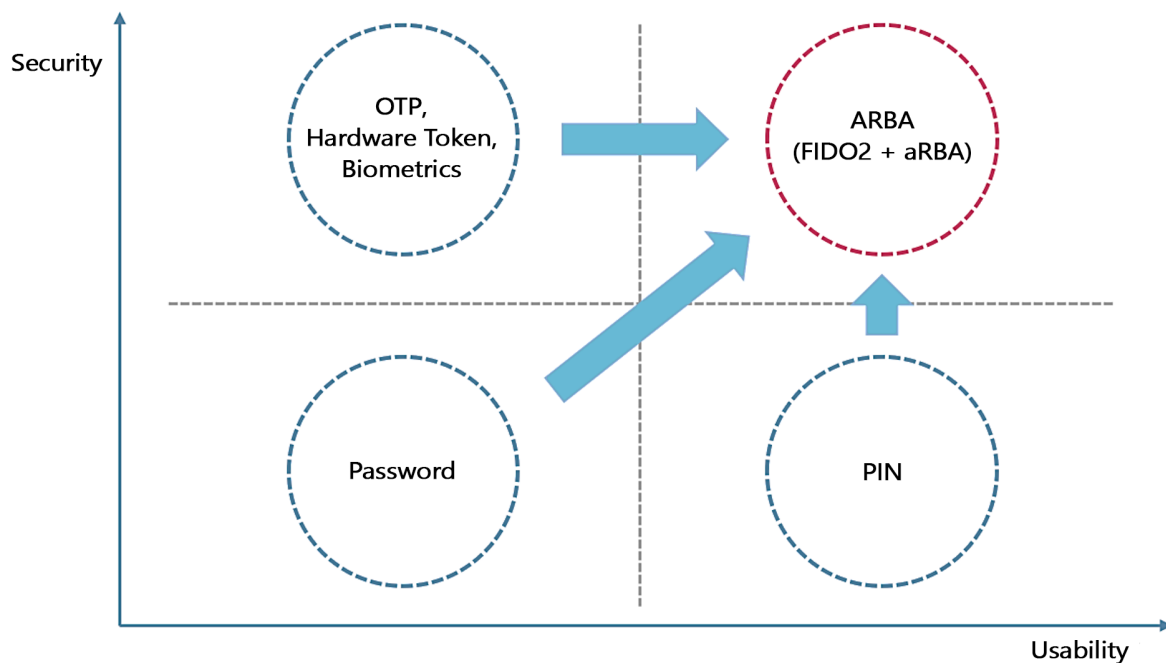


Figure 3.7: Comparison of the proposed ARPA scheme with traditional passwords, PINs, and various 2FA/MFA methods.

At its core, the tables listed below form the foundational pillars of the proposed ARPA scheme. For better security and privacy, any sensitive user information is either hashed using SHA-256 or encrypted using AES-256 prior to being stored in the database.

1. **tblUsers:**

- **user_id:** Unique user identifier (primary key)
- **username:** Username for login
- **email:** User's email address
- **role:** User roles such as admin, user, or guest
- **baseline_risk_score:** Calculated baseline risk score of the user
- **last_login_time:** Timestamp of last successful login
- **last_login_ip:** IP address of last successful login
- **last_login_device_id:** Unique device identifier of last successful login
- **last_failed_login:** Timestamp of last failed login attempt
- **registration_time:** Timestamp of account creation
- **account_status:** Account status such as active, inactive, blocked, deactivated, or suspended

2. **tblDevices:**

- **device_id:** Unique device identifier (primary key)
- **user_id:** Foreign key referencing tblUsers
- **device_type:** Type of device such as laptop, smartphone, desktop, or tablet
- **user_os:** Type of operating system used by the device
- **user_browser:** Type of web browser used by the user
- **device_fingerprint:** Device's unique fingerprint
- **last_seen:** Timestamp of last activity from this device

3. **tblLogin:**

- `login_id`: Unique login attempt identifier (primary key)
- `user_id`: Foreign key referencing `tblUsers`
- `device_id`: Foreign key referencing `tblDevices`
- `timestamp`: Timestamp of the login attempt
- `ip_address`: IP address of the login attempt
- `success`: Boolean value indicating success or failure
- `risk_score`: Calculated risk score for the attempt
- `auth_method`: Method used for authentication such as FIDO2 biometric, FIDO2 possession, PIN, OTP, TOTP, reset or recovery link by email, etc.
- `fallback_auth_requested`: Boolean value indicating if primary or fallback authentication method was requested

4. **tblRiskFactors:**

- `risk_id`: Unique risk factor identifier (primary key)
- `risk_factor`: Name of the risk factor (e.g., geolocation, IP reputation, device type, network anomalies, etc.)
- `weight`: Weight assigned to the risk factor

5. **tblRiskScores:**

- `score_id`: Unique risk score identifier (primary key)
- `user_id`: Foreign key referencing `tblUsers`
- `timestamp`: Timestamp of the risk score calculation
- `risk_score`: Calculated risk score
- `baseline_risk_score`: User's baseline risk score for comparison
- `risk_category`: Classification of the risk (e.g., low, medium, and high)
- `triggering_factor`: Factor(s) that triggered the risk score calculation

6. **tblTrustedDevices:**

- `trusted_dev_id`: Unique trusted device identifier (primary key)
- `user_id`: Foreign key referencing `tblUsers`
- `device_id`: Foreign key referencing `tblDevices`
- `authenticator_id`: Unique identifier for the user's FIDO2 authenticator
- `authenticator_pbk`: The public key associated with the user's FIDO2 authenticator
- `authenticator_type`: Type of FIDO2 authenticator (e.g., security key, smartphone, laptop with embedded biometric scanner like fingerprint or iris, etc.)
- `added_at`: Timestamp when the device was marked as trusted by user
- `last_used_at`: Timestamp of last successful login using this device

7. **tblARPAProfile:**

- `user_id`: Foreign key referencing `tblUsers` (primary key)
- `preferred_authentication_method`: User's preferred FIDO2 authentication method such as biometric device or the possession of a smart card or security.
- `fallback_authentication_method`: User's preferred authentication method such as PIN, OTP, authenticator app, reset or recovery link by email, etc.
- `notification_settings`: User's preferences for receiving notifications (by email, push notification, or by SMS if phone number is stored) in the event of medium and high-risk login attempts
- `baseline_risk_score`: User's baseline risk score
- `allows_biometric_auth`: Boolean value indicating if the user allows biometric authentication
- `allows_precise_geolocation_tracking`: Boolean value indicating if the user allows high-precision geolocation tracking
- `security_mode`: Future iterations ARPA will offer three security settings to give its users more choices — low-security mode, medium-security mode (default), and high-security mode.

8. **tblSessionMgt:**

- `session_id`: Unique session identifier (primary key)
- `user_id`: Foreign key referencing `tblUsers`
- `device_id`: Foreign key referencing `tblDevices`
- `is_device_trusted`: Boolean value indicating if the device in question is 'trusted' by the user (i.e. if `device_id` is present in `tblTrustedDevices`)
- `ip_address`: IP address of the session
- `session_token`: Unique session token
- `timestamp`: Timestamp of session creation
- `last_activity`: Timestamp of last activity within the session
- `baseline_risk_score`: User's baseline risk score

9. **tblGeolocationData:**

- `geo_id`: Unique geolocation data identifier (primary key)
- `user_id`: Foreign key referencing `tblUsers`
- `timestamp`: Timestamp of the geolocation data's collection
- `latitude`: Latitude of the user's location
- `longitude`: Longitude of the user's location
- `accuracy`: Accuracy of the geolocation data (e.g., low, medium, and high)

10. **tblAccRecovery:**

- `rec_id`: Unique account recovery method identifier (primary key)
- `user_id`: Foreign key referencing `tblUsers`
- `rec_type`: Type of recovery method (e.g., reset or recovery link by email, security questions, backup codes, PIN)
- `rec_value`: Value associated with the recovery method (e.g., recovery email addresses, answers to security questions, hashed PIN and backup codes, etc.)

11. **tblBlockedIPs:**

- **blocked_id:** Unique blocked IP address identifier (primary key)
- **ip_address:** Blocked IP address
- **reason:** Reason for blocking (e.g., excessive failed login attempts, known malicious activity)
- **timestamp:** Timestamp of when the IP address was added to the blocked list
- **wildcard_block:** Boolean value indicating if a single IP address in question is blocked or if an entire range of IP addresses (close to the responsible IP address) should be blocked using a wildcard mask.

12. **tblAuditLog:**

- **log_id:** Unique audit log identifier (primary key)
- **user_id:** Foreign key referencing tblUsers
- **timestamp:** Timestamp of the event's occurrence
- **event_type:** Type of event (e.g., login attempt, password change, too many invalid login attempts, account blocked, account recovery, etc.)
- **event_data:** Additional data associated with the event (e.g., IP address, device information, number of invalid login attempts, account lockout duration, etc.)

The above database schema should only be used as a point of reference since the tables herein are not properly normalised and does not account for every single use case scenario. Specific tables may have to be added, implemented differently, or omitted entirely depending on a system's requirements, security priorities, and compliance needs.

This robust and flexible schema attempts to unite aRBA and FIDO2 under one passwordless multi-factor user authentication scheme, ARPA, for a stronger and more user-friendly authentication experience. This adaptable architecture paves the way for a secure and convenient alternative to entering passwords whilst keeping privacy in mind.

3.3.1.5 Pseudocode

Below is a high-level abstract overview of the proposed passwordless multi-factor user authentication scheme, ARPA. Other than the utilisation of FIDO2 authentication as a way for users to authenticate or re-authenticate, the introduction of comparing the calculated risk score of every login attempt with the corresponding user's dynamic baseline risk score is one of the notable attributes of the proposed scheme.

Algorithm 1 An abstract framework for the proposed ARPA scheme, which combines a modified version of the Freeman et al. risk scoring model with FIDO2 authentication.

function ARPA_PASSWORDLESS_AUTHENTICATION (login_attempt, user_id)

Import all necessary libraries and other dependencies for FIDO2 and aRBA

Retrieve user information and risk factors from database:

- Fetch user information (including enrolled FIDO2 credentials and their baseline_risk_score)
- Retrieve static risk factors and their assigned weights
- Retrieve adaptive risk thresholds based on current context (time, user history, threat intelligence, etc.)
- Retrieve hard-coded high_risk_threshold, medium_risk_threshold, and low_risk_threshold values
- Check for account lockout status due to rate limiting:
 - **if** user account is still locked out:
 - block_access_and_notify_user("Account locked out due to multiple failed login attempts")
 - log_authentication_event(user_id, "Attempted to access locked out account", ip_address, datetime)
 - **return**
- **end if**

Retrieve geolocation data for IP address:

- ip_address = extract_ip_address_from_login_attempt(login_attempt)
- geolocation_data = retrieve_geolocation_data(ip_address) // get ISP, ASN, country, other geolocation data, etc.
- is_vpn = check_if_vpn(ip_address) // take action accordingly (choose between blocking them entirely, treating them with caution, or allow them with additional verification, depending on the system's requirements)

(continued next page)

Check for blacklisted IP address:

- wildcard_ip = replace_last_octet_with_wildcard(ip_address)
- **if** wildcard_ip is in blacklisted_ips_table:
 - block_access_and_notify_user("IP address is blacklisted")
 - log_authentication_event(user_id, "Blocked due to blacklisted IP", ip_address, datetime)
 - **return**
- **end if**

Calculate risk score:

- risk_score = modified_freeman_rba_scoring(login_attempt, user_logs, global_logs, num_users, device_fingerprint, geolocation_data, is_vpn) // include all other factors
- trigger = factors_for_increased_risk_score(user_id, risk_score, datetime)

Evaluate risk score and take necessary action:

- Compare the difference between calculated risk_score and baseline_risk_score
- **if** calculated_risk_score <= baseline_risk_score
 - allow_access(user_id, risk_score, datetime)
 - log_authentication_event(user_id, "Successful access due to close proximity to baseline risk score", risk_score, ip_address, datetime)
 - update_database_and_train_system(user_history, acquired_threat_intelligence)
// update the baseline_risk_score as well
 - continue_monitoring_user(user_id) // track user interactions, identify anomalies that could indicate an account compromise, and take action accordingly
- **end if**
- **if** risk_score >= high_risk_threshold:
 - block_access_and_notify_user("High risk detected")
 - log_authentication_event(user_id, "Blocked due to high risk", trigger, risk_score, ip_address, datetime)
 - update_database_and_train_system(user_history, acquired_threat_intelligence)
// update the baseline_risk_score as well
- **else if** risk_score >= medium_risk_threshold and risk_score < high_risk_threshold:
 - fido2_authenticated = request_fido2_authentication(user_id) // function to initiate FIDO2 authentication and return a boolean value after completion
 - log_authentication_event(user_id, "Challenged user to re-authenticate due to medium risk", trigger, risk_score, ip_address, datetime)

(continued next page)

```

- if fido2_authenticated:
    - allow_access(user_id, risk_score, datetime)
    - log_authentication_event(user_id, "Successful FIDO2 authentication", datetime)
    - update_database_and_train_system(user_history, acquired_threat_intelligence)
      // update the baseline_risk_score as well
    - continue_monitoring_user(user_id) // track user interactions, identify anomalies
      that could indicate an account compromise, and take action accordingly
- else:
    - fallback_authentication = request_fallback_authentication(user_id)
      // get user's preferred fallback authentication method (e.g., recovery link via email,
      OTP, PIN, security questions, etc.) and return a boolean value after completion
    - log_authentication_event(user_id, "FIDO2 authentication failed, challenged
      user to re-authenticate with fallback authentication method", datetime)
    - if fallback_authentication:
        - allow_access(user_id, risk_score, datetime)
        - log_authentication_event(user_id, "Successful login with fallback
          authentication", datetime)
        - update_database_and_train_system(user_history, acquired_threat_intelligence)
          // update the baseline_risk_score as well
        - continue_monitoring_user(user_id) // track user interactions, identify anomalies
          that could indicate an account compromise, and take action accordingly
    - else:
        - block_access_and_notify_user("FIDO2 and fallback authentication failed")
        - log_authentication_event(user_id, "Failed FIDO2 and fallback
          authentication", datetime)
        - update_database_and_train_system(user_history, acquired_threat_intelligence)
          // update the baseline_risk_score as well
    - end if
  - end if
- else:
    - allow_access(user_id, risk_score, datetime)
    - log_authentication_event(user_id, "Successful access due to low risk", risk_score,
      ip_address, datetime)
    - update_database_and_train_system(user_history, acquired_threat_intelligence)
      // update the baseline_risk_score as well
    - continue_monitoring_user(user_id) // track user interactions, identify anomalies
      that could indicate an account compromise, and take action accordingly
  - end if
end function // can be modified to be called recursively until the expiration or termination of login session

```

3.3.2 User Testing (Experimentation)

To analyse what the general public think about passwords as well as hardware-backed biometric authentication in relation to perceived security, convenience, and privacy, a sample size of $n = 32$ volunteers were asked to interact with the ARPA prototype for some amount of time and then provide their feedback by answering a carefully crafted set of closed-ended survey questions. Their attitude towards combining FIDO2 and aRBA was noted as well.

- **Participant Recruitment:** To ensure a good sample size of the target audience, a healthy mix of men and women volunteers were recruited by taking factors such as age, technical proficiency, and diversity into consideration for maximising the generalisability of findings.
- **Prototype Development:** As delineated in Subsection 3.3.1 of this thesis, a basic, working prototype of the proposed ARPA was developed by incorporating the two core elements of the multi-factor authentication mechanism, FIDO2 and aRBA.
- **Testing Environment:** A controlled testing environment was designed and set up to simulate real-world scenarios. The participants were provided with specific tasks to perform using a dummy web application that incorporated an early prototype version of the ARPA scheme. Afterwards, they were asked to answer a series of questions to gain some insight into their experience of using the proposed user authentication scheme.
- **Testing Procedure:** Participants tested the ARPA prototype and then completed a series of close-ended survey questions designed to capture their feedback on usability, security perception, and overall experience of the proposed scheme.
- **Data Analysis:** Finally, the data and feedback obtained by surveying users were used to analyse and evaluate the effectiveness as well as

user acceptance of the proposed ARPA scheme. The extrapolated data gave some valuable insights into the potential of this scheme and laid a foundation for future development efforts.

3.3.3 Survey Questionnaire

As mentioned previously, in order to capture the responses and opinions of the user testing group, a series of closed-ended survey questions were administered to the volunteers using Google Forms for its ease of use and for its secure data transmission as well as storage options. These questions allowed to gauge user perceptions, satisfaction, and the acceptance rate of the proposed user authentication scheme. Thus, volunteers were asked to immediately answer the question shortly after their interaction with the prototype system to ensure that their responses capture the immediate perceptions and experiences of using ARPA.

- **Questionnaire Design:** Closed-ended survey questions were designed to align with the research objectives and quantify users' perceptions and experiences of using the ARPA scheme. The questions therein covered aspects such as its feasibility, usability, security, privacy, and overall user satisfaction.
- **Validation:** Pre-testing of the survey was performed to ensure clarity and relevance of the questions being asked. Moreover, Cronbach's alpha was also calculated and considered for assessing the overall reliability of the survey questions as it takes into account the average correlation between all pairs of items in the set. A higher value indicates that the items are more closely related and that the measure is more reliable.

3.3.4 Ethical Considerations

Although the study did not receive any official (or unofficial) approval from relevant institutional review boards, the research plan has still adhered to basic ethical guidelines and informed consent was obtained from all participants. Strict measures were implemented to protect participants' privacy, including anonymisation of all collected data and secured storage. Their names and other personally identifying information were either not collected or immediately discarded.

3.4 Data Analysis

The data collected from prototype testing and survey responses underwent quantitative analysis using descriptive statistics. The analysis focused on key metrics related to the performance, security, and user acceptance of the novel authentication scheme with special attention to usability and privacy in addition to the level of security it provides.

However, due to a lack of time, the analysis did not involve segmenting users based on demographics or technical proficiency to identify patterns of acceptance and challenges. Other limitations of the study are mentioned in the subsequent section of the thesis.

3.5 Research Limitations

Ideally, the proposed user authentication scheme should be developed, tested, and refined in a systematic and iterative manner as it would allow for continuous improvement based on user feedback which, in turn, would ensure that the proposed user authentication scheme evolves to meet users' needs more effectively.

However, this could not be done in this case due to time and broader resource constraints such as the prolonged participation of more volunteers or testers and creating a more expansive testing environment which would ultimately require more funding and use of various technologies. Hence, a more streamlined approach was taken instead. Further iterative development and testing can certainly be performed to deliver an effective replacement for traditional password-based user authentication systems.

Moreover, detailed performance metrics such as system responses, authentication success/failure rates, response times, errors or anomalies encountered, and various other user actions, could have been logged and graphed during the experiment for subsequent in-depth analysis.

Lastly, another potential limitation is the combination of relatively small sample size, controlled conditions for user testing, and the basic nature of the prototype, which may have limited the generalisability of the findings to real-world contexts. That being said, these aspects were carefully designed to ensure precision and accuracy in the data collected. The basic nature of the prototype, though a potential limitation, still serves as a solid foundation upon which future developments and refinements can be built as it lays the groundwork for more extensive studies that can delve into broader contexts, thus enhancing the applicability of the findings to a wider range of real-world situations.

Chapter 4

Results and Discussion

4.1 Overview

This chapter draws attention to the insights obtained from this study’s exploration into the feasibility, benefits, and challenges of integrating FIDO2 into aRBA to conceive the ARPA user authentication scheme. The development of a basic prototype served as a foundational milestone as it provided a tangible proof-of-concept for the envisioned integration of two complementary technologies.

Moreover, the volunteer feedback gathered through a closed-ended survey also offered valuable perspectives on user experiences as it shed light on to the practical implications of the combination of the two core technologies. The findings underscore the potential benefits of enhanced security through aRBA’s robust and intelligent authentication mechanisms as well as FIDO2’s interoperability and usability benefits, as validated by the overwhelmingly positive quantitative feedback from the volunteers.

The adopted research methodology, incorporating both technical implementation and user-centric feedback, contributed to a holistic understanding of the proposed integration's dynamics. This chapter navigates through these nuanced outcomes to provide a comprehensive perspective on the viability and implications of the ARPA scheme, offering valuable insights for the broader landscape of aRBA and FIDO2 user authentication systems.

4.2 Bridging the Gap

As established previously, the aim of this endeavour was to create a novel and robust user authentication scheme that incorporates FIDO2 into an aRBA scheme and explore the feasibility and effectiveness of combining the two technologies in an attempt to deprecate the use of passwords for good.

Although it is possible that similar solutions may already exist in the real world in one form or another, perhaps developed independently for catering specific needs of various organisations, their existence remains largely undocumented in formal research papers and other publicly available resources. This lack of documentation poses a significant challenge for anyone who is seeking comprehensive insights into existing practices and solutions into combining the two technologies.

Therefore, the proposed solution represents an opportunity to bridge the gap between practical implementations and academic knowledge. By documenting the intricacies of the proposed passwordless multi-factor user authentication scheme, which incorporates FIDO2 with aRBA, this thesis aims to contribute not only to the academic discourse but also to the broader cybersecurity community. The documentation of this solution can serve as a valuable resource for researchers, cybersecurity enthusiasts, and organisations looking to understand, replicate, or enhance their existing user authentication solutions.

4.3 User Testing (Experimentation)

4.3.1 Overview

32 participants with diverse demographics and technology proficiency levels volunteered to test a basic, working proof-of-concept version of the proposed ARPA scheme. Prior to the experiment, they were asked to answer ten (10) baseline questions and were then briefed about the ARPA scheme by highlighting how it works, what it aims to achieve, and how users can benefit from such a scheme. They were then asked to complete a series of tasks using a purpose-built dummy web application that incorporates a prototype version of the ARPA scheme to simulate real-life situations whilst trying to access a system online.

These tasks were designed to assess the general usability, understandability, and overall user experience of the ARPA scheme in different simulated scenarios where users might need to authenticate and re-authenticate themselves due to a change in certain conditions.

Afterwards, the participants were asked to complete a post-experiment survey. The survey consisted of 22 closed-ended questions designed to obtain quantitative data on their thoughts, perceptions, and experiences with the ARPA scheme prototype.

4.3.2 Prelude

Shortly after the volunteers answered a series of baseline questions and prior to their participation in the experiment, the primary concept and innerworkings of the proposed ARPA scheme, specifically its two underlying technologies, aRBA and FIDO2, were explained to them using a series of simplified figures and publicly available videos on the subject matter. The videos played, totalling a runtime of nearly 16 minutes, were as follows:

- "What is Risk-based Authentication and what are its benefits?"¹
- "What is WebAuthn?"²
- "WebAuthn from W3C and FIDO Alliance - What You Need To Know"³
- "Understanding passkeys in 4 minutes"⁴

Some of the more non-technical figures used herein were shown to the participants with the inclusion of Figure 4.1 below to help them visualise how the proposed passwordless authentication scheme works and how they could benefit from it in their everyday lives.

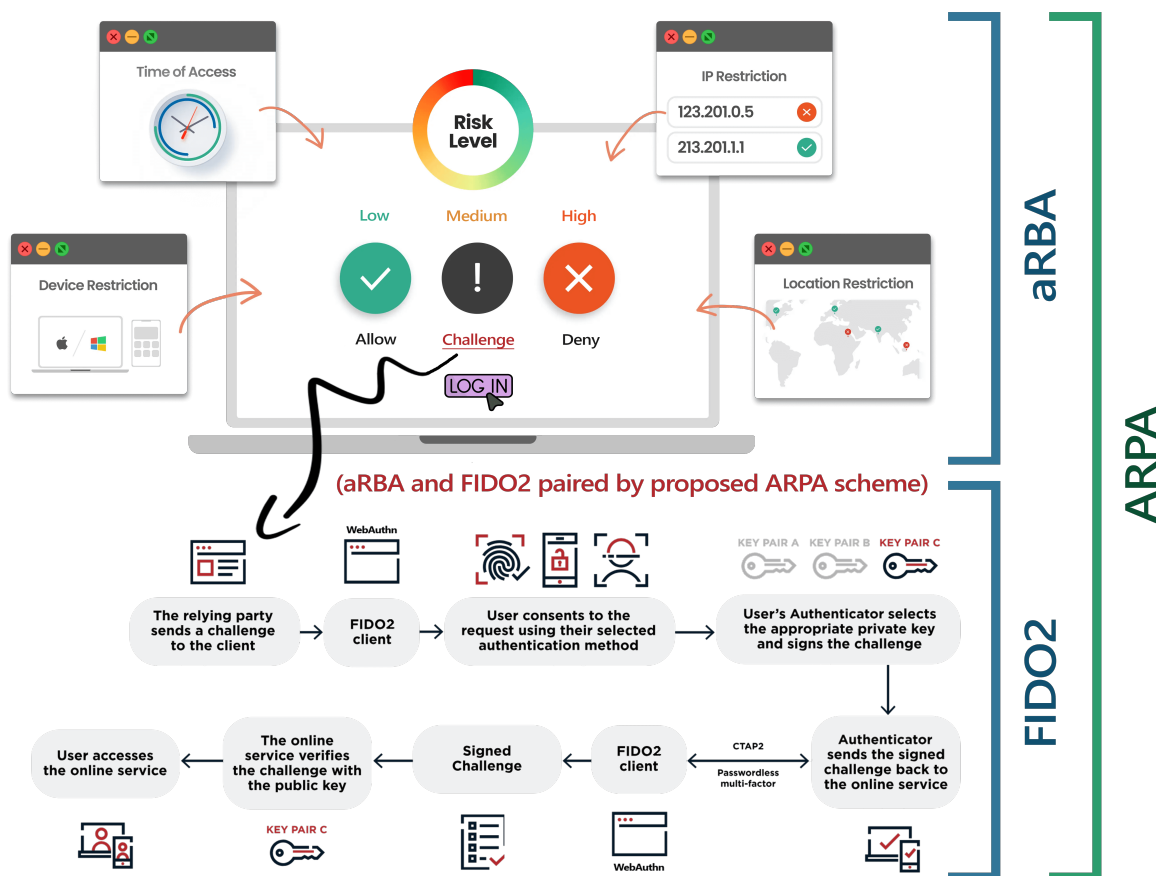


Figure 4.1: A high-level overview of the login process in the proposed ARPA scheme.

¹ <https://www.youtube.com/watch?v=NMxe3z-3-hE>

² <https://www.youtube.com/watch?v=zJPNuORkvvk>

³ <https://www.youtube.com/watch?v=F3IGS5HaMuc>

⁴ <https://www.youtube.com/watch?v=2xdV-xut7EQ>

In the meantime, the aRBA component (risk engine) of the proposed ARPA scheme was trained using a trimmed and modified version of the RBA dataset made available on GitHub by Wiefling et al.⁵ This involved simulating account takeover attacks as well as seemingly normal login attempts into dummy user accounts tied to the purpose-built web application with the help of a browser automation tool known as Selenium, although Cypress and Playwright were also considered but were eventually ruled out. This was later complemented by real-life login attempts made by actual users with and without VPN, in addition to other simulated scenarios that are described in subsequent subsections of this chapter.

Although the dummy web application was designed with a focus on user-friendliness to enhance its appeal among individuals with limited technical expertise, a brief walk-through and guidance were still provided to ensure a smooth onboarding experience for users of all technical backgrounds and to help the entire sample size fully utilise the proposed user authentication scheme's key features.

Moreover, volunteers were asked to use their own smartphones, laptops, and security keys to further test as well as prove the prototype system's compatibility with different devices, form factors, operating systems, web browsers, and regional settings in addition to gathering feedback on the system's usability and functionality on varying platforms and real-world conditions.

4.3.3 User Registration Process

The experiment began by instructing participants to register an account on a dummy web application that utilises the ARPA prototype as the default user authentication scheme as opposed to traditional password-based authentication systems. Users were asked to enter a username and then sign up us-

⁵ <https://github.com/das-group/rba-dataset#study-reproduction>

ing their preferred FIDO2 authentication method, which were mostly limited to being software-based due to the prevalence of smartphones and the convenience of having a FIDO2 authenticator readily available on a device they likely already carry with them at all times. This involved users unlocking their smartphones using a PIN code or by entering their biometric information, and it was made abundantly clear that these private information never left their devices. Users also had the choice of setting their device as a "trusted device" to allow future login attempts with as little restriction as possible.

Moreover, users with YubiKey security keys were instructed to register their key using NFC or by inserting it into the USB/Lightning port of their device (smartphone or laptop). Some keys also support biometric authentication for additional security against theft, but none of the participants had one on their person. However, it is important to note that hardware-based FIDO2 authenticators offer increased security and better tamper resistance, so security keys could be a better choice for users who require the highest level of security.

Regardless of the type of FIDO2 authenticator is chosen, hardware or software-based, the user's device generates a pair of private and public keys, and the latter is signed with an attestation certificate prior to being used to sign the challenge from the RP Server. The signed challenge and the public key are then sent to the RP Server for storing the users' login credentials and associating it with their respective accounts. The use of public-key cryptography and attestation certificates ensures that the user's private key is never shared with the online service, and the use of a unique key pair for each device, service, and user account prevents cross-site scripting and various other common attacks.

The generated key pair is unique for the local device, online service, and user's account. This means that even if a user has multiple FIDO2 authen-

ticators, each authenticator will generate a unique key pair for each online service that the user registers with. Although the prototype ARPA scheme currently lacks the ability to support the use of multiple FIDO2 authenticators, it still demonstrates just how secure, private, and convenient FIDO2 authentication can be for end users.

During the registration process, users were also prompted to enter their email address and also set up their preferred authenticator app as a fallback authentication measure in the event that the primary means of authenticating a user failed or is unavailable. This would also allow for additional security and account recovery if it gets locked out due to too many invalid login attempts. The version of the prototype used during the experiment lacked the ability for users to set PIN codes or answers to security questions, but the registered email address was used to notify suspicious activities to users as well as providing OTPs (recovery codes) to regain access to temporarily locked-out accounts. Users were briefed about this during the experiment.

4.3.4 User Login Process

4.3.4.1 Baseline Logins

This portion of the experiment was comprised of volunteers logging into their newly created user accounts and accessing a few preset sections of the dummy web application in several successions under usual scenarios to set a baseline for the risk engine component of the prototype scheme.

- Participants performed successful logins under normal circumstances using their usual devices, network environment (private WiFi), locale settings, and web browser combinations.
- The system gathered baseline data on login context (IP address, geolocation, device fingerprint, etc.) and assigned low risk scores, which led to a lower baseline risk score.

- The use of FIDO2 authenticators reduced within the first few login attempts as the prototype ARPA system was now in a position to ascertain if the same user was attempting to log in or access the login-protected pages of the dummy web application with very little delay (2-3 seconds waiting time).
- Nevertheless, users were also asked to attempt logging in using their previously set fallback authentication method instead of their FIDO2 authenticator for simulating a scenario where the user's FIDO2 authenticator is unavailable due to being forgotten elsewhere, lost, stolen, or damaged. This was done to see how well the system handled the transition from FIDO2 authentication to fallback authentication.

4.3.4.2 Testing Risk Scenarios

Contextual data gathered from users' activities as well as the results from the automated Selenium script earlier served to establish a good baseline for the risk engine component of the proposed user authentication scheme.

To test the prototype system's ability to mitigate, if not entirely prevent, account takeover attacks, volunteers were asked to access their account under a variety of different simulated scenarios. This included using different WiFi networks, devices, web browsers, time zone and time of day. Readily available VPNs and a browser extension called ScriptSafe were used to obscure as well as spoof information like the public IP address, geolocation, user agent string, and various device/browser fingerprinting attributes to simulate login or access attempts from unfamiliar places and devices. All the scenarios tested are listed below.

- **Network Changes:** Users switched between different WiFi and mobile networks, including networks from different ISPs located elsewhere in the same country, which led to potential medium risk scores.

- **VPN Usage:** Instructed users to toggle between different VPN/proxy connections set to different countries, triggering higher risk scores based on location discrepancies.
- **Device Switching:** Users switched between their phones and laptops for different login/access attempts. This resulted in varying risk scores depending on device familiarity and historical usage.
- **Browser Switching:** Users used different web browsers on the same device, causing low to medium risk scores due to contextual changes.
- **User Agent Spoofing:** Instructed users to spoof user agents during different login attempts, which triggered medium to high risk scores due to discrepancies with baseline login data.
- **Screen Resolution Changes:** Users changed the screen resolutions on their laptops between their login/access attempts, which also resulted in medium to high risk scores as screen resolutions do not normally change so frequently.
- **Time Zone and Time of Day:** Simulated login attempts from different time zones at randomised times of the day for triggering a variety of risk scores.

As the proposed ARPA scheme continuously monitored every login attempt and user sessions following a successful login, it adjusted the level of scrutiny applied to each user based on calculated risk scores and the subsequent level of risk determined by the scheme in real time.

While low risk scores warranted access without any hindrance, in cases where the risk was deemed to be non-negligible, the system either prompted the user for FIDO2 re-authentication or block the login/access attempt altogether for medium and high-risk levels respectively. Table 4.1 summarises the results of the study's simulated scenarios during the experiment.

Table 4.1: A truncated summary of the actions taken by the proposed ARPA scheme captured during a segment of the experiment.

User ID	Baseline Risk Score	Calculated Risk Score	Risk Level	Action Taken	Login Attempts	Scenario	Authenticator Used	Fallback Authentication Method Used
U002	0.27	0.23	Low	Allowed Access	1	Registered device (smartphone)	N/A	N/A
U005	0.39	0.54	Medium	FIDO2 challenge	1	Unknown device (laptop)	Roaming (smartphone; Biometric)	N/A
U007	0.31	0.83	High	Access Blocked & Email Sent	2	Suspicious or blacklisted IP address	N/A	N/A
U009	0.15	0.12	Low	Allowed Access	1	Registered device (laptop)	N/A	N/A
U011	0.28	0.32	Medium	FIDO2 challenge	1	Registered device (smartphone)	Platform (smartphone; Biometric)	N/A
U018	0.37	0.50	Medium	FIDO2 challenge	2	Different ISP and location	Roaming (security key; NFC)	authenticator app (OTP)
U021	0.43	0.56	Medium	FIDO2 challenge	2	Unknown device (smartphone)	Roaming (security key; USB)	N/A
U024	0.18	0.41	Medium	FIDO2 challenge	1	Public WiFi network	Platform (laptop; Windows Hello)	N/A
U027	0.23	0.12	Low	Allowed Access	1	Registered device (smartphone)	N/A	N/A
U028	0.16	0.37	Medium	FIDO2 challenge	2	Unknown device (laptop)	N/A	authenticator app (OTP)
U031	0.79	0.88	High	Access Blocked & Email Sent	3	Unknown device (laptop)	N/A	email (OTP)
U032	0.29	0.63	Medium	FIDO2 challenge	1	VPN usage	Platform (laptop; PIN verification)	N/A

The prototype scheme dynamically calculates a higher risk score in the event that a non-negligible discrepancy or anomaly is detected, and this score is then compared with the baseline score to automatically determine if more stringent security measures are required and take a preset course of action such as requesting re-authentication or entirely blocking access to the account. This allows the proposed user authentication scheme to effectively mitigate the risk of unauthorised access whilst simultaneously providing a seamless and convenient user experience for an account's intended user as identification factors do not normally have sudden and erratic fluctuations.

Furthermore, some curious testers also tried logging into the dummy web application with the username of other testers against the experimental protocol, but the prototype ARPA scheme was effortlessly able to flag the login attempts as suspicious and took the necessary action accordingly.

4.3.4.3 FIDO2 Re-authentication

The proposed ARPA scheme initiates a FIDO2 (re-)authentication challenge for medium-level risks, which requires the user to use their registered authenticator to verify their identity. This additional layer of security helps ensure that the user is indeed the legitimate account holder and deters any unauthorised access from occurring by requiring them to authenticate using a strong, second factor such as biometric identification or the possession of an authenticator like a security key or a trusted device.

Users therefore have the choice between using platform authenticators such as their trusted laptops and smartphones or by using external (roaming) authenticators like their security keys and smartphones as illustrated in Figures 4.2 and 4.3 respectively (next page).

This makes the proposed user authentication scheme 2FA by default, which is further complemented by an adaptive risk engine that evaluates several identifiable factors and maintains a separate user profile for each account

holder in a way that enables it to differentiate between each user.



Figure 4.2: An illustration of the use of a security key in the proposed ARPA scheme.

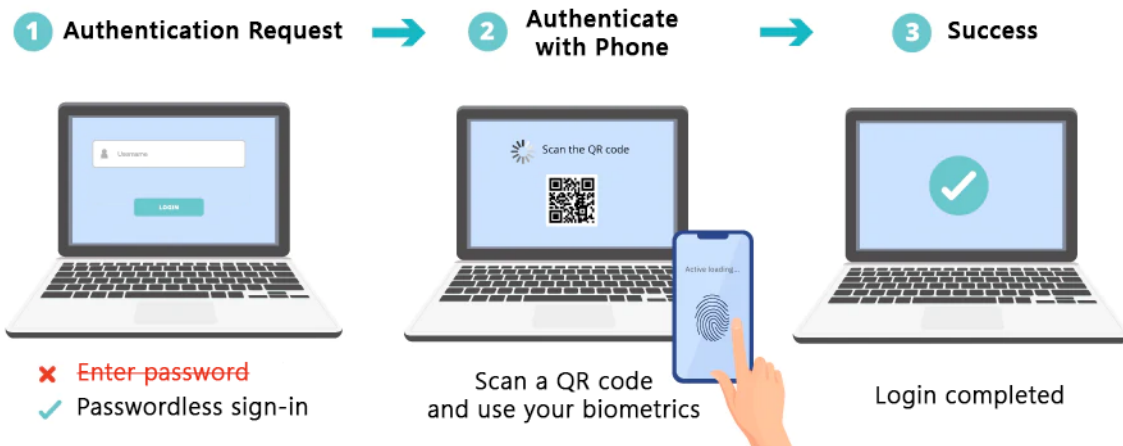


Figure 4.3: An illustration of the use of smartphones as a roaming authenticator in the proposed ARPA scheme.

As hinted previously, smartphones have the added benefit of not only being ubiquitous but also being able to serve as both platform and roaming authenticators. When used as the latter, users can sign in by scanning a QR code and then simply authenticate with biometric identification. Thus, users are provided with the flexibility to choose between platform authenticators or external (roaming) authenticators for this re-authentication process.

Screenshots of the prototype version of the ARPA scheme that was used during the experiment may be found in the appendices section of the thesis.

Table 4.2: Non-exhaustive list of FIDO2 certified devices and fallback authentication methods supported by the proposed ARPA scheme.

Category	Login Device/Mechanism	Underlying Authentication Technology
Platform Authenticator	Smartphone	Biometric verification (Face ID / Touch ID in Apple devices)
	Smartphone	PIN verification
	Smartphone	Bluetooth (proximity authentication)
	Laptop	Biometric verification (Windows Hello or Face ID / Touch ID in Apple devices)
	Laptop	PIN verification
	All-in-One Desktop PC	Biometric verification (Windows Hello or Face ID / Touch ID in Apple devices)
	All-in-One Desktop PC	PIN verification
Roaming Authenticator	Smartphone	Biometric verification
	Smartphone	PIN verification
	Smartphone	Bluetooth (proximity authentication)
	Smartwatch	Bluetooth (proximity authentication)
	Security Key	USB / NFC
	Contactless Smart Card	NFC (predominantly) / RFID
Fallback Authentication	Authenticator App (for OTP)	TOTP (predominantly) / HOTP
	Email	OTP
	Email	Account Recovery Link (not implemented yet)
	Email	PIN set by user (not implemented yet)
	Email	User-defined security questions (not implemented yet)

As seen in Table 4.2 above, users have a variety of 2FA options when it comes to picking their primary passwordless method of logging in, so they are not limited to just one or two choices. Moreover, users are strongly advised to set up a fallback authentication method for being able to access their respective accounts in the event of unforeseen circumstances that render their primary means of logging in unavailable.

4.3.4.4 Purpose of the Experiment

This experiment aimed to evaluate the effectiveness of the prototype ARPA scheme by analysing user experience and system performance across various login scenarios and keeping track of how well the proposed user authentication scheme balances security, usability, and privacy with the unification of FIDO2-based authentication and aRBA technology.

The aim of this experiment was to evaluate the effectiveness of ARPA in a controlled environment by testing its adaptive risk-based authentication (aRBA) capabilities with different login scenarios and the affect it had on user experience. This was done by examining its ability to distinguish between legitimate users and potentially fraudulent login attempts under varying conditions.

As the goal of this endeavour was to use aRBA and deprecate the use of passwords in favour of biometric and possession-based authentication, users were asked to use only FIDO2-based biometrics and security keys during the experiment to authenticate or re-authenticate themselves with a fallback authentication method of their choice.

4.3.4.5 Post-experiment Survey

Following the conclusion of the experiment, which involved 32 participants testing a basic, working proof-of-concept version of the ARPA scheme, the volunteers were asked to complete a survey of 22 targeted questions to gather valuable feedback on their overall experience with the proposed password-less authentication scheme.

Responses from the users were then analysed for gaining insights into their overall experience and perception of the ARPA scheme in terms of security, privacy, and ease of use. It also allowed to identify areas for improvement in the scheme's design and user experience. Hence, it laid down the foundation for further development and optimisation of the prototype.

4.4 Discussion of Results

This section attempts to analyse the valuable user feedback obtained through the closed-ended survey conducted with 32 volunteers who interacted with the ARPA prototype and were later asked to answer a series of questions to gather relevant and quantifiable feedback from potential users.

It explores user perceptions, preferences, and challenges encountered during the user testing process. By examining user experience and acceptance levels, this section aims to gauge the practicality and user-friendliness of incorporating FIDO2 into an aRBA scheme, providing insights into potential adoption barriers and areas for improvement. All of this is a crucial part of the user-centred design approach, which refers to a series of processes that focus on putting users and their needs at the center of a product's design and development.

4.4.1 Survey Questions & User Responses

4.4.1.1 Baseline Questions

Participants were first asked to answer ten (10) preliminary questions prior to taking part in the testing of the ARPA prototype. This included answering a select few demographic questions to better understand the representativeness of the experiment's sample.

Asking baseline and demographic questions before a survey is not just a formality, but a vital step in ensuring the accuracy, reliability, and generalisability of the research findings. It allows researchers to understand the context of their recorded data, identify potential biases, draw meaningful conclusions, and tailor their insights to specific subgroups within the population.

The questions asked are mentioned below along with the percentage of selection each option received.

- **SQ:01[Prelim]** — “Please state your gender.”
 - **Male — 59.4% (19)**
 - Female — 40.6% (13)
- **SQ:02[Prelim]** — “Please state your age.”
 - **18–30 years old — 40.6% (13)**
 - 31–45 years old — 31.3% (10)
 - 46–60 years old — 25.0% (8)
 - 60+ years old — 3.1% (1)
- **SQ:03[Prelim]** — “Please state your education level.”
 - Attended school — 6.3% (2)
 - Completed high school — 9.4% (3)
 - Diploma holder — 6.3% (2)
 - **Some college credit, but no degree awarded — 40.6% (13)**
 - Bachelor’s degree — 21.9% (7)
 - Master’s degree — 12.5% (4)
 - PhD — 3.1% (1)

- **SQ:04[Prelim]** — “How proficient are you with technology in general, particularly when it comes to adapting to new systems?”
 - Very Proficient — 3.1% (1)
 - Proficient — 28.1% (9)
 - **Somewhat Proficient — 53.1% (17)**
 - Inefficient — 9.4% (3)
 - Very Inefficient — 6.3% (2)

- **SQ:05[Prelim]** — “Do you think passwords alone can adequately safeguard your online accounts?”
 - Yes — 15.6% (5)
 - **No — 84.4% (27)**

- **SQ:06[Prelim]** — “Does it concern you when you hear about large data breaches and password leaks?”
 - **Yes — 90.6% (29)**
 - No — 9.4% (3)

- **SQ:07[Prelim]** — “Do you find using biometric authentication (i.e. using your fingerprint, eye (iris/retina), face, voice, etc.) much quicker and convenient than entering passwords?”
 - **Yes — 96.9% (31)**
 - No — 3.1% (1; the participant wears glasses and has calloused fingers, which made it harder for them to use biometric authentication)

- **SQ:08[Prelim]** — “Do you have any privacy concerns regarding using biometric authentication?”
 - **Yes — 71.9% (23)**
 - **No — 28.1% (9)**

- **SQ:09[Prelim]** — “How often do you keep your phone in your person?”
 - **Always — 71.9% (23)**
 - **Nearly Always — 15.6% (5)**
 - **Most Times — 9.4% (3)**
 - **Sometimes — 3.1% (1)**
 - **Rarely — 0.0% (0)**

- **SQ:10[Prelim]** — “Do you mind carrying a physical security key (that takes the form factor of a smart card or a USB thumb drive) on your person at all times?”
 - **Yes — 18.8% (6)**
 - **No — 81.3% (26)**

4.4.1.2 Targeted Questions

As mentioned previously, 32 participants were asked to answer a series of questions after they volunteered to test a basic, working proof-of-concept version of the ARPA scheme. Based on the results obtained from the baseline questions, the respondents were primarily comprised of young adults and middle-aged men and women with varying degrees of technical expertise with their responses predominantly being positively in favour of ARPA.

A pilot testing of the survey questions (SQs) was performed with a small subset of the total sample size of $n = 32$ group for ensuring that relevant questions were being asked in an easy-to-understand manner. However, due to the closed-ended nature of the questions, participants were unable to provide any additional feedback or suggestions for improving future builds of the ARPA scheme. This seems like a promising opportunity for future work. In any case, the survey questions asked are listed below along with the percentage of selection each option received from the participants.

1. Effectiveness Evaluation:

- **SQ:01[Eff]** — “Compared to entering passwords or your other usual login methods, how easy and secure did you feel while using ARPA to log in on a scale of 1-5?”
 - 1 (Very Easy & Secure) — 21.9% (7)
 - **2 — 56.3% (18)**
 - 3 (Neutral) — 15.6% (5)
 - 4 — 6.3% (2)
 - 5 (Very Difficult & Insecure) — 0.0% (0)
- **SQ:02[Eff]** — “On a scale of 1-5, how much did the ARPA scheme impact your overall login experience in terms of convenience, security, and privacy?”
 - 1 (Significantly Improved) — 18.8% (6)
 - **2 — 65.6% (21)**
 - 3 (Neutral) — 12.5% (4)
 - 4 — 3.1% (1)
 - 5 (Significantly Worsened) — 0.0% (0)

2. Integration Challenges:

- **SQ:03[Int]** — “How often do you encounter technical difficulties while using FIDO2 or similar biometric/possession-based user authentication methods with existing applications or devices?”
 - Very Frequently — 0.0% (0)
 - Frequently — 3.1% (1; the participant wears glasses and has calloused fingers, which made it harder for them to use biometric authentication)
 - Sometimes — 12.5% (4)
 - **Rarely — 59.4% (19)**
 - Very Rarely — 25.0% (8)
- **SQ:04[Int]** — “How satisfied are you with the fallback authentication measures if you were unable to log in with your biometrics or trusted device due to an integration issue or some other unexpected issue?”
 - Very Satisfied — 25.0% (8)
 - **Satisfied — 56.3% (18)**
 - Neutral — 12.5% (4)
 - Dissatisfied — 3.1% (1)
 - Very Dissatisfied — 3.1% (1)

3. Privacy and Regulatory Compliance:

- **SQ:05[Pri]** — “On a scale of 1-5, how confident are you that ARPA protects your privacy and data? Keep in mind that your biometric data never leaves your device and nearly all of the processing is done locally in the case of the FIDO2-based authentication.”
 - 1 (Very Confident) — 21.9% (7)
 - **2 — 53.1% (17)**
 - 3 (Neutral) — 15.6% (5)
 - 4 — 6.3% (2)
 - 5 (Very Unconfident) — 3.1% (1)
- **SQ:06[Pri]** — “On a scale of 1-5, how comfortable are you with the amount of contextual, behavioural, and environmental data collected and used by the ARPA scheme knowing that they are collected and stored safely to verify if it is really you trying to log in?”
 - 1 (Very Comfortable) — 18.8% (6)
 - **2 — 56.3% (18)**
 - 3 (Neutral) — 15.6% (5)
 - 4 — 6.3% (2)
 - 5 (Very Uncomfortable) — 3.1% (1)

4. User Experience and Satisfaction:

- **SQ:07[Use]** — “On a scale of 1-5, how would you rate the impact of the ARPA scheme on your user experience and satisfaction compared to traditional password-based and 2FA/MFA methods?”

- 1 (Very Satisfied) — 25.0% (8)
 - **2 — 53.1% (17)**
 - 3 (Neutral) — 15.6% (5)
 - 4 — 6.3% (2)
 - 5 (Very Dissatisfied) — 0.0% (0)
- **SQ:08[Use]** — “What is your overall perception and attitude towards the ARPA scheme?”
 - Very Positive — 28.1% (9)
 - **Positive — 56.3% (18)**
 - Neutral — 12.5% (4)
 - Negative — 3.1% (1)
 - Very Negative — 0.0% (0)
 - **SQ:09[Use]** — “Would you prefer using ARPA for future login attempts?”
 - **Yes — 90.6% (29)**
 - No — 9.4% (3)

5. Security Evaluation:

- **SQ:10[Sec]** — “On a scale of 1-5, how secure do you think ARPA is compared to traditional password-based authentication for your online user accounts?”
 - **1 (Much More Secure) — 53.1% (17)**
 - 2 — 37.5% (12)
 - 3 (Neutral) — 6.3% (2)
 - 4 — 3.1% (1)

- 5 (Much Less Secure) — 0.0% (0)
- **SQ:11[Sec]** — “Can you think of any potential security risks associated with using the ARPA scheme?”
 - Yes — 31.3% (10)
 - No — **68.8% (22)**

6. Scalability and Performance:

- **SQ:12[Sca]** — “On a scale of 1-5, how quickly and smoothly did the ARPA scheme respond to your login attempts compared to other authentication methods you use regularly?”
 - **1 (Very Fast & Smooth) — 75.0% (24)**
 - 2 — 15.6% (5)
 - 3 (Neutral) — 6.3% (2)
 - 4 — 3.1% (1)
 - 5 (Very Slow & Glitchy) — 0.0% (0)
- **SQ:13[Sca]** — “On a scale of 1-5, how strongly do you think ARPA would be suitable for use in systems with a large number of users?”
 - 1 (Strongly Agree) — 40.6% (13)
 - **2 — 46.9% (15)**
 - 3 (Neutral) — 9.4% (3)
 - 4 — 3.1% (1)
 - 5 (Strongly Disagree) — 0.0% (0)

7. User Adoption and Education:

- **SQ:14[Ado]** — “Was there any aspect of the ARPA scheme that you found confusing or challenging while using it for the first time?”
 - Yes — 40.6% (13)
 - No — **59.4% (19)**
- **SQ:15[Ado]** — “How helpful were the instructions provided to you for using the ARPA scheme on a scale of 1-5?”
 - 1 (Very Clear & Helpful) — 31.3% (10)
 - **2 — 50.0% (16)**
 - 3 (Neutral) — 15.6% (5)
 - 4 — 3.1% (1)
 - 5 (Confusing & Unhelpful) — 0.0% (0)
- **SQ:16[Ado]** — “Would you appreciate having additional information and training materials readily available on screen or on demand to make you feel more comfortable using the ARPA scheme?”
 - Yes — **84.4% (27)**
 - No — 15.6% (5)

8. Long-Term Viability and Future Trends:

- **SQ:17[Via]** — “On a scale of 1-5, how confident are you that ARPA will remain secure and relevant in the future, considering emerging technologies and evolving cyber threats?”

- 1 (Very Confident) — 34.4% (11)
 - **2 — 40.6% (13)**
 - 3 (Neutral) — 21.9% (7)
 - 4 — 3.1% (1)
 - 5 (Very Unconfident) — 0.0% (0)
- **SQ:18[Via]** — “Are you aware of any future trends in authentication methods that might impact the relevance and continued use of the ARPA scheme?”
 - Yes — 9.4% (3)
 - **No — 90.6% (29)**

9. Comparative Analysis:

- **SQ:19[Ana]** — “Compared to most other authentication methods, how would you rate the ARPA scheme in terms of security and ease of use on a scale of 1-5?”
 - 1 (Very Secure & User-friendly) — 21.9% (7)
 - **2 — 56.3% (18)**
 - 3 (Neutral) — 15.6% (5)
 - 4 — 6.3% (2)
 - 5 (Less Secure & User-friendly) — 0.0% (0)
- **SQ:20[Ana]** — “If you have used other passwordless authentication methods, how would you compare the ARPA scheme to those alternatives?”
 - Much Better — 34.4% (11)
 - **Better — 40.6% (13)**

- Similar — 25.0% (8)
- Worse — 0.0% (0)
- Much Worse — 0.0% (0)
- **SQ:21[Ana]** — “Have you ever heard or read about adaptive risk-based authentication (aRBA) or (Fast IDentity Online v2) FIDO2 prior to volunteering to use the ARPA prototype?"
 - Yes — 28.1% (9)
 - No — **71.9% (23)**
- **SQ:22[Ana]** — “Would you be interested in participating in future testing of ARPA prototypes?"
 - Yes — **87.5% (28)**
 - No — 12.5% (4)

4.4.2 Mapping of Questions

The survey of 10 + 22 questions featured a variation of the commonly used Likert scale, which offers a quantifiable way of measuring positive and negative opinions or attitudes from a sample of users regarding a particular statement or question. All 32 respondents were asked to choose the option that closely corresponded with how they felt about a certain statement or question to gauge an accurate representation of their experience with the ARPA scheme prototype.

With the exception of SQ:21[Ana] and SQ:22[Ana], the table below (next page) maps each survey question (SQ) to one or more corresponding research questions (RQs) with the aim to find or extrapolate answers to each of the RQs. The ten baseline or preliminary questions are also not listed here as they were asked to serve a different purpose.

Table 4.3: Mapping between the research questions (RQs) and the questions in the survey (SQs) along with the status of each RQ.

RQ	SQ	RQ Status
1. RQ:Eff[01+02]	SQ:01[Eff]	Answered
2. RQ:Eff[02]	SQ:02[Eff]	Answered
3. RQ:Int[01+02]	SQ:03[Int]	Partially Answered
4. RQ:Int[02]	SQ:04[Int]	Partially Answered
5. RQ:Pri[01]	SQ:05[Pri]	Answered
6. RQ:Pri[02]	SQ:06[Pri]	Answered
7. RQ:Use[01]	SQ:07[Use]	Answered
8. RQ:Use[01+02]	SQ:08[Use]	Answered
9. RQ:Use[02]	SQ:09[Use]	Answered
10. RQ:Sec[01]	SQ:10[Sec]	Answered
11. RQ:Sec[02]	SQ:11[Sec]	Partially Answered
12. RQ:Sca[01]	SQ:12[Sca]	Partially Answered
13. RQ:Sca[02]	SQ:13[Sca]	Partially Answered
14. RQ:Ado[01]	SQ:14[Ado]	Partially Answered
15. RQ:Ado[02]	SQ:15[Ado]	Partially Answered
16. RQ:Ado[02]	SQ:16[Ado]	Partially Answered
17. RQ:Via[01]	SQ:17[Via]	Partially Answered
18. RQ:Via[02]	SQ:18[Via]	Partially Answered
19. RQ:Ana[01]	SQ:19[Ana]	Answered
20. RQ:Ana[01+02]	SQ:20[Ana]	Partially Answered

This survey focused on concise closed-ended survey questions to effectively elicit answers to the research questions while minimising respondent burden. Each survey question directly maps to at least one research question, as illustrated in Table 4.3 above. Each SQ was designed to address specific research questions (RQs) that were listed earlier, either by combining insights from multiple questions or by using Likert scales for quantitative analysis. This approach aims to gather comprehensive data while keeping the survey concise and quicker as well as easier for participants to answer.

For example, SQ:01[Eff] combines RQ:Eff[01] and RQ:Eff[02] by asking users to rate both security and convenience on a single scale. Similarly, both SQ:15[Ado] and SQ:16[Ado] were asked to answer RQ:Ado[02] by gathering specific feedback on overcoming adoption barriers by educating the general public about ARPA and its inner workings (FIDO2 and aRBA).

4.4.3 Key Findings

The overall response from 32 participants offer an overwhelmingly positive feedback towards the proposed ARPA scheme. This is evident across various aspects, which are presented in a concise manner in Table 4.4 below.

Table 4.4: Summary of the most common responses received for 10 + 22 questions asked to a sample of 32 users of the ARPA scheme prototype following its testing.

Survey Question (SQ)	Most Common Response
Baseline Questions	
SQ:01[Prelim]: Gender	"Male" — 59.4% (19)
SQ:02[Prelim]: Age	"18–30 years old" — 40.6% (13)
SQ:03[Prelim]: Education	"Some college credit, but no degree awarded" — 40.6% (13)
SQ:04[Prelim]: Tech Proficiency	"Somewhat Proficient" — 53.1% (17)
SQ:05[Prelim]: Passwords Deemed Secure	"No" — 84.4% (27)
SQ:06[Prelim]: Data Breach Concern	"Yes" — 90.6% (29)
SQ:07[Prelim]: Biometric Preference	"Yes" — 96.9% (31)
SQ:08[Prelim]: Biometric Privacy Concern	"Yes" — 71.9% (23)
SQ:09[Prelim]: Phone Accessibility	"Always" — 71.9% (23)
SQ:10[Prelim]: Security Key Preference	"Yes" — 81.3% (26)
Targeted Questions about ARPA	
SQ:01[Eff]: Ease of Use & Security	"Easy & Secure" — 78.2% (25)
SQ:02[Eff]: Overall Impact	"Much Improved" — 84.4% (27)
SQ:03[Int]: FIDO2/Biometric Difficulties Faced	"Rarely" — 84.4% (27)
SQ:04[Int]: Fallback Authentication Satisfaction	"Satisfied" — 81.3% (26)
SQ:05[Pri]: Privacy Confidence	"Confident" — 75.0% (24)
SQ:06[Pri]: Contextual Data Collection Concern	"Comfortable" — 75.1% (24)
SQ:07[Use]: Impact on User Experience	"Satisfied" — 78.1% (25)
SQ:08[Use]: Overall User Perception	"Positive" — 84.4% (27)
SQ:09[Use]: Future Use Preference	"Yes" — 90.6% (29)
SQ:10[Sec]: Security Compared to Passwords	"Much More Secure" — 90.6% (29)
SQ:11[Sec]: Perceived Security Risks	"No" — 68.8% (22)
SQ:12[Sca]: Speed & Smoothness	"Very Fast & Smooth" — 90.6% (29)
SQ:13[Sca]: Suitability for Large Systems	"Agree" — 87.5% (28)
SQ:14[Ado]: Initial Confusion	"No" — 59.4% (19)
SQ:15[Ado]: Instruction Clarity	"Clear & Helpful" — 81.3% (26)%
SQ:16[Ado]: Additional Information/Training	"Yes" — 84.4% (27)
SQ:17[Via]: Relevance & Security in Future & Relevance	"Confident" — 75.0% (24)
SQ:18[Via]: Awareness of Future Authentication Trends	"No" — 90.6% (29)
SQ:19[Ana]: Security & User-friendliness	"Secure & User-friendly" — 78.2% (25)
SQ:20[Ana]: Comparison to Other Passwordless Methods	"Much Better" — 75.0% (24)
SQ:21[Ana]: Prior Knowledge of aRBA/FIDO2	"No" — 71.9% (23)
SQ:22[Ana]: Interest in Future ARPA Testing	"Yes" — 87.5% (28)

Overall summary of the survey's findings is as follows:

- **Ease of use and security:** Most participants (78.2%) rated their login experience as "easy and secure" when compared to entering passwords, using password managers, and other usual login methods.
- **Overall impact:** Over 84.4% reported a significant improvement in their login experience in terms of convenience, security, and privacy with ARPA.
- **Integration challenges:** Only 3.1% encountered frequent difficulties with FIDO2-based or biometric authentication in existing applications. However, given the relatively low sample size, this figure will likely increase if more people are exposed to the ARPA scheme, which primarily relies on biometric and possession-based authentication. Nevertheless, over 80% of the participants expressed their satisfaction with fallback authentication measures.
- **Privacy and regulatory compliance:** Over 75% expressed confidence in ARPA's data privacy practices and were also comfortable with their data being collected, processed, and used for automatically confirming their identity without much or any effort on their part. Most participants were willing to make the trade-off between better privacy and added convenience by opting to share these details for not having to log in as many times.
- **User experience and satisfaction:** Nearly 80% found ARPA to positively impact their user experience compared to traditional login methods, with 84.4% having a positive overall perception of the proposed user authentication scheme. Over 90% of the participants even expressed their interest to try ARPA in their everyday lives with their actual user accounts if given the choice.

- **Security evaluation:** A staggering 90.6% believe that ARPA is more secure than traditional password-based authentication, and only 31.3% identified potential security risks. This figure, however, is not negligible and it warrants further research to be performed on minimising security risks by as much as possible.
- **Scalability and performance:** Nearly all participants (90.6%) rated their login attempts to be fast and smooth, and most (87.5%) strongly believe that ARPA would be suitable for large user systems as well.
- **User adoption and education:** While 40.6% faced initial confusion, 81.3% found the instructions clear and helpful. Moreover, 84.4% of the participants stated that having access to additional information and training resources would be very much appreciated. It may also be noted that nearly 70% of the participants stated that they were unaware of the underlying FIDO2 and aRBA technologies prior to volunteering to use the ARPA prototype. It would certainly help with the scheme's adoption rate to build more awareness about the technologies that power it.
- **Long-term viability and future trends:** Three-quarters of the participants are confident that ARPA will remain secure and relevant in the future, and 87.5% of users even expressed their interest to participate in further testing of ARPA prototypes.
- **Comparative analysis:** Nearly 80% rated ARPA as secure and user-friendly compared to other user authentication methods, and most (75%) consider it better than alternative passwordless methods due to the inclusion of aRBA, which significantly reduces the number of times a user has to re-authenticate themselves whenever their session expires.

As per the survey findings, the prototype ARPA scheme received a strong acceptance from a diverse group of users with varying demographics and technology experience levels. Its user-friendly and secure nature, coupled with its potential for scalability and adaptability, presents a very promising prospect for the future of secure and convenient user authentication.

4.5 Limitations

4.5.1 Limited Sample Size

Admittedly, the detailed analysis performed in this thesis is based on a relatively small sample size of 32 participants even though various efforts were made to ensure an adequate amount of variety in the participants and the validity of the feedback obtained from them. Factors such as gender, age, education, and level of technical expertise were considered to yield additional insights from a diverse sample of potential end-users.

Although the results and feedback obtained may not seem very significant given the sample size of $n = 32$, they are still worthy of consideration as even small samples can sometimes reveal important trends or patterns that warrant further investigation with a larger sample size in future studies. Therefore, larger-scale studies are needed to re-confirm the findings of this study and generalise them to a broader population.

4.5.2 Lack of Raw Performance Metrics

Vital data from users' interaction with the proposed ARPA scheme such as system responses, authentication success/failure rates, response times, errors or anomalies encountered, and various other user actions, could have been logged during the experiment and then graphed for performing an in-depth analysis of the strengths, viability, and performance of the proposed scheme.

4.5.3 Lack of Open-Ended Questions

The quantitative results obtained herein from the closed-ended survey should be complemented with more qualitative interview data by asking them a series of open-ended questions to close the research gap. A few such questions to ask volunteers in future testing of the ARPA scheme are listed below. These would encourage them to provide detailed feedback and insights for further improvements to be made. Experts in the field should also be consulted for their professional opinion on the feasibility of this novel user authentication scheme.

1. "What new features or improvements would make future versions of ARPA even more appealing for you to use?"
2. "How easily can ARPA be integrated into existing systems and applications?"
3. "Any potential security vulnerabilities or attack vectors to address in the ARPA scheme?"
4. "What aspects of ARPA do you think makes it stand out compared to traditional password-based authentication schemes or other 2FA/MFA methods?"
5. SQ:03[Int] may be modified to ask what technical difficulties a user typically faces while using FIDO2 or other similar biometric/possession-based authentication methods with existing applications or devices.
6. SQ:11[Sec] may be modified to learn what potential security risks have the potential to be associated with the ARPA scheme.
7. SQ:14[Ado] may be modified to list which aspects of the ARPA scheme were found to be confusing or challenging while being used for the very first time.

8. SQ:18[Via] may be modified to record future trends in authentication methods from knowledgeable users to get a better understanding of the impact they might have on the relevance and continued use of the ARPA scheme.
9. SQ:20[Ana] may be modified to learn how the ARPA scheme compares against other passwordless authentication methods in terms of convenience, security, and privacy, including any features or changes that it would benefit from having.
10. The inclusion of a “Please share any additional feedback or suggestions you have for improving the ARPA scheme.” question at the end of the survey.

4.5.4 Lack of Behavioural Data

While closed-ended questions can help gather opinions, they cannot capture actual user behaviour during interaction with the prototype ARPA scheme. This makes it difficult to assess its usability in real-world scenarios and identify specific pain points or areas for further improvement.

Moreover, measuring user experience (UX) goes beyond simple satisfaction ratings. With a small sample and closed-ended questions, it is challenging to quantify and analyse UX aspects like learnability, efficiency, and memorability.

4.5.5 Partially Answered Research Questions

Given the basic nature of the ARPA prototype and the relatively low sample size of testers, several research questions remain partially answered, and are therefore inconclusive due to the limitations of the sample size and survey design.

For instance, questions such as RQ:Int[02], RQ:Sec[02], RQ:Sca[01+02], RQ:Ado[01+02], RQ:Via[01+02], and RQ:Ana[02] require further research, testing, and experimentation to be performed for obtaining a definitive answer to each of those research questions.

4.5.6 Potential for Overlooked Issues

With a small sample, it is possible that important usability or security challenges might be overlooked or wrongly evaluated, thereby requiring further investigation with a larger and more diverse group of users as 32 participants may prove to be inadequate in providing diverse usage patterns for identifying potential issues, rare scenarios, or edge cases that could arise in real-world deployments.

4.6 Summary

The adaptive risk engine of the proposed ARPA scheme utilises factors such as device and browser fingerprinting, IP address familiarity, geolocation, geo-velocity, past login information, behavioural biometrics, and network anomalies to continuously monitor every single login attempt as well as subsequent user sessions following a successful login. It identifies suspicious login attempts with a high degree of accuracy, assigns an appropriate risk level, and then takes the most appropriate course of action.

The experiment described herein provides a framework for testing the core functionalities of the proposed ARPA scheme in simulated real-life scenarios in a controlled environment.

The results of the experiment showed that a user authentication scheme that combines aRBA with FIDO2 re-authentication is a highly effective way to protect users against account takeover attacks whilst simultaneously ensuring their privacy and convenience as it allows for, inter alia:

- **Real-time & adaptive response to threats:**

- The system's ability to continuously monitor user sessions and adjust the level of scrutiny in real time allows it to respond quickly to possible account takeover attacks as well as various other forms of threats and attacks.
- Theoretically, this means that even if a threat actor is able to compromise a user's account or trusted device, the system would still be able to quickly detect any anomalous change in behaviour or some other contextual factor and take the recommended course of action to prevent any further damage.

- **Improved user experience:**

- By tailoring the authentication process to the individual user's risk level, the system is able to provide a more seamless and frictionless experience for low-risk users, thereby improving the overall user experience and satisfaction.
- Reduces the need for multiple, repetitive authentication processes, which may lead to something commonly known as "MFA fatigue."
- FIDO2 authenticators can be used to securely store and manage user credentials, thereby eliminating the need for users to remember multiple complex and/or unique passwords or use password managers.
- FIDO2 authentication is typically performed with minimal interruption to the user's workflow. Users simply sign in with their preferred way of authentication only when the adaptive risk analysis engine component detects a non-negligible change in factors used to identify the intended user of an account.

Based on available information and the user feedback received, the following results may be extrapolated about the proposed ARPA scheme:

Table 4.5: Comparison of the ARPA scheme with popular user authentication schemes.

Feature	Scheme 1 (S1: Pwd)	Scheme 2 (S2: MFA)	Scheme 3 (S3: RBA)	Scheme 4 (S4: FIDO2)	ARPA
Security	! - Moderate if implemented properly, but vulnerable to phishing, brute-forcing, stolen, and leaked	! - High, but still vulnerable to phishing and MFA fatigue attacks	! - High if implemented properly; same vulnerability as S1 and S2	✓ - Stronger; phishing-resistant	✓ - Strongest; combines strengths of S3 and S4
Convenience	! - Simple to use, but difficult to remember and type complex passwords	X - Inconvenient; involves multiple steps	! - Moderate; still requires MFA for some logins	✓ - Convenient; easier to use biometrics/security keys (inherently 2FA)	✓ - More convenient; only requires FIDO2 re-auth on medium risk
UX	✓ - Easiest	X - Can be inconvenient, frustrating, and time-consuming	! - Can be inconvenient for users forced into MFA	✓ - Smooth and seamless experience	✓ - Smooth and seamless experience
Speed	✓ - Fast; only password entry	X - Slow; involves multiple steps	! - Can be slow if MFA is triggered	✓ - Moderate to fast; requires biometrics or security key interaction	✓ - Fastest if no re-auth required; same as S4 otherwise
Privacy	X - Low to moderate; heavily depends on password storage policies; subject to theft and leakage	! - Moderate; OTPs and push notifications can be intercepted	! - Moderate (varies between implementations); user data used for risk assessment is stored on server	✓ - High; biometric information and other encrypted information are stored locally	✓ - Moderate to high; has strengths of S4; balances privacy with security (use of encryption and hashing wherever applicable); data collected strictly for risk assessment
Acceptability	✓ - Widely accepted and preferred due to unprecedented familiarity	! - Not as widely accepted (low adoption rate); a good number of users dislike MFA due to added inconvenience	✓ - Acceptable since not as inconvenient as S2; some users may find the risk assessment methodology intrusive	✓ - Growing acceptance, but not universally familiar yet	✓ - Has great potential as it combines familiar and modern approaches from S3 and S4 (mostly); flexible approach caters to users' preferences; still requires education
Accuracy	! - Moderate to high; prone to typos if entered manually; can be auto-filled	! - Similar to S1; typos can occur while entering OTPs; can mistakenly confirm or deny login when prompted via push notification	! - Similar to S2; risk assessment may not always be accurate; reduced odds of MFA-related mistakes from occurring	✓ - Very high due to biometrics and security keys being inherently unique for each user	✓ - Similar to S3 and S4; aims for high accuracy through adaptive risk assessment and FIDO2

(continued next page)

Phishing Resistance	X - Highly susceptible to phishing	! - Users can still be tricked into becoming victims of phishing attacks	! - Similar to S2, but much lower risk of occurrence	✓ - Practically phishing resistance	✓ - Similar to S4 (primary authentication) and S3 (fallback auth)
Continuous Authentication	X - Absent	X - Absent	✓ - Present in aRBA, but necessarily in RBA	X - Absent	✓ - Present
False Positive Rate	✓ - Low	! - Subject to user error and type of MFA	! - Low to moderate; stringent risk assessment may flag innocuous activity	✓ - Very low; biometrics and security keys are inherently unique	✓ - Low; adaptive risk assessment helps reduce false positives, but it is still possible; combines the strengths of S4
False Negative Rate	X - High; vulnerable to phishing, password leaks, and brute-forcing	! - Subject to user error and type of MFA	! - Low to moderate; lax risk assessment may miss suspicious activity	✓ - Very low; biometrics and security keys are difficult to forge/spoof; small chance for biometric/key failure	✓ - Low (similar to S4); adaptive risk assessment helps reduce false negatives, but it is still possible
Scalability	✓ - Highly scalable; no additional infrastructure required	✓ - Scalable, but requires cloud-based solutions for OTP/push	✓ - Scalable, but requires managing risk assessment logic for optimal resource and data usage	✓ - Scalable, but requires FIDO2 server infrastructure as well as compatibility between devices and existing infrastructure	✓ - Scalable, similar to S3 and S4
Implementation Complexity	✓ - Very low; no additional infrastructure required	! - Moderate; requires integration with multiple channels for OTP/push	! - Moderate; similar to S2, but also increased due to the incorporation of risk assessment logic	! - Moderate; requires FIDO2 server integration	! - Moderate; combines the complexities of S3 and S4
Implementation Cost	✓ - Very low; no additional costs	✓ - Low to moderate; requires infrastructure and maintenance for chosen MFA methods	! - Moderate; same as S2 in addition to the development of the risk analysis engine	! - Moderate; requires FIDO2 integration and a compatible infrastructure	! - Moderate to high (S3+S4); requires a higher initial investment, but has the potential for long-term cost savings
Other Considerations	! - Prone to password fatigue and other attacks mentioned previously; requires user education on password security	! - Requires user to manage multiple credentials; vulnerable to social engineering attacks	! - Requires balancing security, privacy and convenience	! - Limited to devices with biometrics/keys; may not be suitable for all applications	! - Aims to address limitations of other schemes, but adds complexity and cost for developers; requires user education on FIDO2 and aRBA

- **Scheme 1 (Pwd):** A commonly used password-only solution where only long random alphanumeric strings of both cases are accepted.

Example: <https://www.goodreads.com/>

- **Scheme 2 (MFA):** A traditional 2FA/MFA solution that either sends OTP codes and push notifications to phones or sends OTP codes to user's email for every login attempt. Users must go through it in addition to entering their password or PIN code.

Example: <https://store.steampowered.com/>

- **Scheme 3 (RBA):** A risk-based authentication solution that forces users to use complex passwords and/or MFA (essentially an extended implementation of Schemes 1 and 2) for signing in due to a medium or high risk being detected.

Example: <https://www.amazon.com/>

- **Scheme 4 (FIDO2):** Exclusive use of biometric authentication or security keys for each login attempt with the aid of FIDO2 authenticators or passkeys. Most popular websites today are still continuing to use Schemes 1, 2, and 3, but 4 is also gradually starting to see mainstream implementation and use.

Example: <https://www.google.com/>

- **ARPA:** It is evident that the proposed passwordless multi-factor user authentication scheme requires more data collection and analysis compared to other schemes (sparing RBA/aRBA), which can potentially raise some privacy concerns. However, it mitigates this by using privacy-preserving techniques and only collecting data relevant to the risk assessment.

Furthermore, combining FIDO2 and aRBA comes with the caveat of increased complexity to implementation and cost compared to other simpler user authentication schemes.

While each scheme has its strengths and weaknesses, the proposed ARPA scheme presents a compelling combination of security, convenience, and privacy as illustrated in Figure 4.4 below.

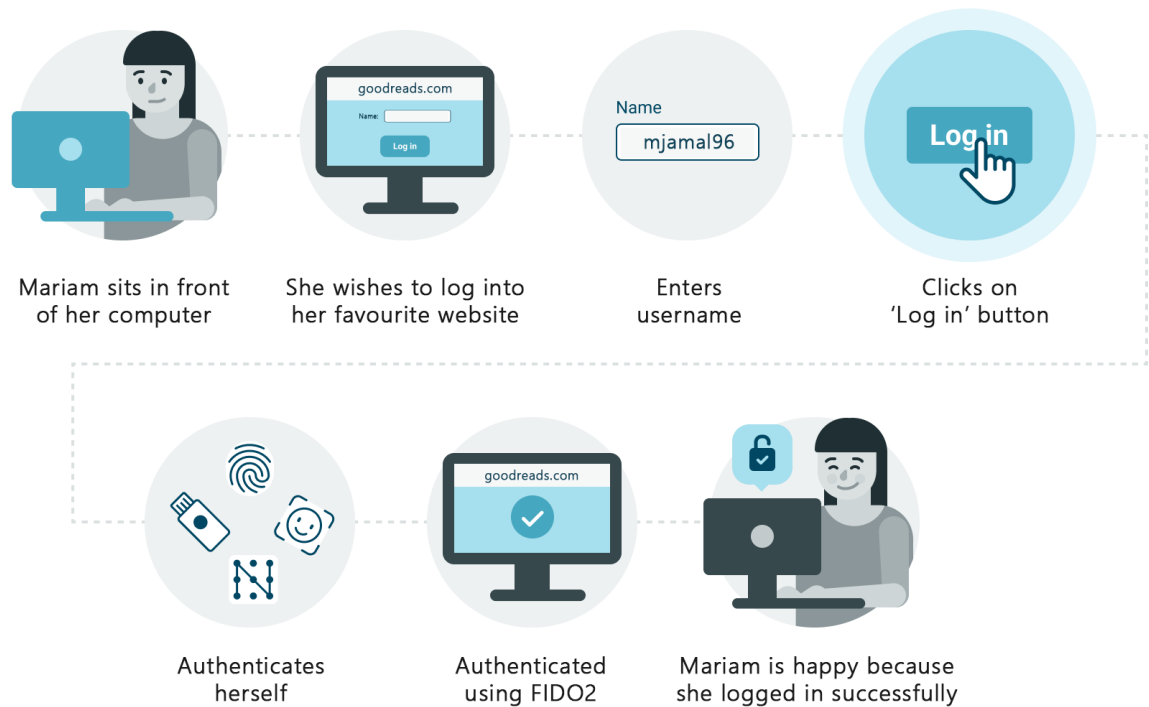


Figure 4.4: A very simplified illustration of the login process in the proposed ARPA scheme.

The ARPA scheme is highly resistant to unauthorised access because it is able to detect and respond to suspicious activities in real time by either requesting FIDO2 re-authentication or completely restricting access as deemed appropriate based on the level of risk detected. By leveraging strong authentication methods like FIDO2 and adapting security measures based on real-time risk assessment, the proposed user authentication scheme offers a robust, reliable, and flexible solution for user authentication.

However, as mentioned previously, implementing such a scheme requires careful consideration of its added complexity, cost, scalability, and potential impact on user experience.

Chapter 5

Conclusion and Recommendations

5.1 Final Overview

This thesis attempted to delve into the technical aspects of integrating FIDO2 into aRBA and discuss the feasibility of a proposed passwordless multi-factor user authentication scheme that combines the two technologies to offer a more comprehensive scheme which aims to provide a better balance of security, usability, and privacy. The proposed scheme was given the name ARPA as it attempts to unify the strengths of aRBA and FIDO2 (passwordless authentication). Moreover, it may also be noted that the industry standard for passwordless authentication is now known as "Passkeys."

5.1.1 Recap of ARPA's Underlying Technologies

FIDO2 is a set of open standards that enables strong authentication without the use of passwords. It is based on strong public-key cryptography and it

primarily relies on biometric and possession-based authentication to confirm a user's identity while attempting to log into a variety of online services such as including web applications, mobile apps, and cloud services that support FIDO2 login. It may be a relatively new standard for authenticating users, but it is slowly starting to see mainstream adoption and use due to a strong backing from industry leaders.

FIDO2 provides a number of advantages over traditional password-based authentication such as, but certainly not limited to:

- **Stronger security:** FIDO2 credentials are stored on the user's device and are not shared with the server. This makes them much more difficult to steal or compromise than passwords. They also greatly reduce the number and severity of phishing as well as social engineering attacks and various other kinds of attacks that typically plague password-based authentication schemes.
- **Improved usability:** It can be argued that FIDO2 authentication is much easier and faster than most other popular user authentication methods. Users can simply tap their phone or insert their security key to authenticate. There is no need for the tedious task of remembering strong, unique passwords or changing them after a period of them.
- **Increased privacy:** FIDO2 does not require users to share their personal information with servers, which helps protect their privacy. Moreover, the nature of biometric and possession-based authentication schemes make them phishing resistant by design. They are also immune to threats that typically apply to passwords. This allows them to safeguard users' accounts and personal information more effectively. Users do not have to worry about having their accounts taken over.

The need for an open and interoperable user authentication scheme becomes apparent when compatibility must be guaranteed between different

platforms with vastly different hardware, software, architecture, and operating systems. The FIDO2 authentication standard achieves this compatibility with the help of WebAuthn API and the CTAP2 protocol.

On the other hand, aRBA is a type of authentication that dynamically adapts to the risk of a given login attempt. It uses a variety of factors such as a user's location, device, and behaviour to assess the likelihood of a fraudulent login attempt occurring and then determine the appropriate level of authentication required. In the proposed ARPA scheme, aRBA is implemented in a way that aims to maximise security and user convenience by essentially operating in three modes:

- **Low Risk:** Allowing unhindered access to a user if all identification factors positively hint towards it being the intended user of an account.
- **Medium Risk:** Requesting re-authentication with preferred FIDO2 authentication method if any non-negligible discrepancy or anomaly is detected such as a sudden change of device, geolocation (but within same country), operating system, user agent, etc.
- **High Risk:** Deny access to the account and trigger a temporary account lockout with an alert being sent to the user's registered email address notifying of a likely fraudulent login attempt due to maximum attempts being reached in a short period of time with the option to regain access to the account.

By combining FIDO2 and aRBA, the proposed ARPA scheme aims to provide a more comprehensive authentication solution that offers a better balance of security, usability, and privacy. The inherently 2FA/MFA scheme uses FIDO2 for strong authentication and aRBA to adapt the level of authentication to the risk of a given transaction such as a new login attempt or resuming a user session after a period of inactivity. This allows the proposed scheme to greatly minimise the risks of session token hijacking as well

as the theft of saved user credentials and cookies in web browsers, thereby keeping users' online accounts safe and secure against emerging threats that antiquated authentication schemes simply cannot protect against.

5.1.2 Conclusion

This endeavour explored the feasibility and development of a basic, working proof-of-concept of the ARPA passwordless authentication scheme, and analysed the challenges encountered during its implementation stage and the subsequent user testing process. It provides a strong foundation and valuable insights for interested individuals or organisations looking to implement ARPA — or a similar scheme that incorporates aRBA and FIDO2 (re-)authentication — into their existing user authentication systems.

The design of the experiment herein provides a good starting point for evaluating the effectiveness of the ARPA scheme as a viable candidate for realising a future where passwordless authentication becomes the new norm.

By addressing the limitations of the study's current design and ramping up future development efforts by incorporating user feedback and all other pertinent information obtained throughout this entire endeavour, the proposed ARPA scheme can be further improved and optimised with each iteration until it is ready for real-world deployment in a live environment.

Shifting to passwordless authentication requires overcoming public doubts and misconceptions about FIDO2 or even biometric and hardware possession-based authentication schemes in general. Decades of reliance and use of passwords create a long road to user adoption, but the potential security, privacy, and convenience gains are worth the effort to bid adieu to passwords for good and drastically limiting the attack vectors that can potentially be exploited by cybercriminals to take over users' accounts and compromise their privacy.

5.2 Recommendations

5.2.1 Build upon a Strong Foundation

The design of the experiment provides a fairly comprehensive framework for testing the ARPA prototype with simulated real-life scenarios in a controlled environment. However, by combining user feedback with the data obtained so far and the information herein, more extensive experiments can be designed to gather further valuable insights for guiding future development efforts into creating a more refined and well-optimised version of the proposed ARPA scheme that is suitable for real-world deployment. Complementing it with objective performance metrics would certainly yield even better results. Therefore, future iterations of the ARPA prototype and its user testing process can build upon this existing framework to:

- **Collect and analyse raw performance metrics:** This will provide valuable insights into the usability, efficiency, and security of the proposed authentication scheme.
- **Identify potential security vulnerabilities:** Performance metrics and extensive user testing can help to identify areas where the ARPA scheme may be vulnerable to certain kinds of attacks and help bring overlooked or previously untested edge cases scenario to light.
- **Incorporate open-ended questions into the survey:** This will allow participants to provide more detailed feedback and insights on their experience with the scheme. A better, more fuller conclusion can be drawn by complementing the quantitative findings with qualitative data to guide future development efforts for a more refined and optimised version of the ARPA scheme.

- **Provide evidence to support design decisions:** Objective performance metrics can be used to support design decisions and justify the choices made in the development of the authentication scheme. Incremental improvements require iterative development and continuous testing to gather as well as incorporate valuable user feedback.
- **Address partially answered research questions:** As hinted above, future studies and experimental design will have to be refined for being able to address the partially answered research questions in an effective manner and provide valuable insights into the usability, efficiency, and security of the ARPA scheme.

5.2.2 Incorporate Machine Learning

In the interest of preparing the ARPA scheme for real-world deployment, the next logical step would be to explore the possibility of incorporating machine learning for enhanced risk assessment and more intelligent risk scoring. This would require investigating into advanced techniques like anomaly detection based on risk prediction models that utilise factors such as historical login patterns, device characteristics, and behavioural biometrics to make this novel user authentication scheme more robust and sophisticated in identifying suspicious activities by giving it the ability to learn and improve its risk assessment capabilities over time.

Although the inclusion of machine learning will considerably increase the time, cost, and complexity for implementing the ARPA scheme into live environments, it may prove to be a necessary trade-off for making the scheme much quicker and more accurate for being able to successfully tackle future threats.

5.2.3 Addressing Low Awareness and Adoption Rates

Another issue to address with the proposed multi-factor passwordless user authentication scheme is the seemingly low awareness and adoption rates of its two core technologies, FIDO2 and aRBA, among the general public.

A 2023 study by the FIDO Alliance found that a good majority of security professionals are aware of FIDO2, but public awareness still remains to be lagging behind. Furthermore, its mainstream adoption still faces hurdles such as lack of user awareness and education as well as limited support for legacy systems. However, major tech companies like Google, Microsoft, Samsung, and Apple are continuing to integrate it into their platforms to help improve its awareness and adoption among the general population. Now it is up to popular websites and applications to support FIDO2 authentication by implementing the ARPA scheme, for instance.

On the other hand, the concept of aRBA is not new, but public awareness of its implementation remains to be on the lower end of the spectrum. Many users encounter it indirectly through services that adjust security based on factors like location or device, but they may not be explicitly aware of the underlying technology. Its widespread adoption depends on balancing security with user experience as well as taking privacy concerns into consideration and ensuring transparency in how the risks are assessed.

5.2.4 Opt for Self-Hosting

Throughout the duration of the experiment performed as a part of this thesis, the dummy web application (with the ARPA scheme prototype) was hosted on a readily available free hosting plan offered by 000webhost. However, due to the nature of the testing process involving the usage of automation scripts and VPNs as well as numerous attempts to test the capabilities of the aRBA risk engine component, the web hosting provider flagged the project

for suspicious activities and that subsequently led to its automatic deletion and the suspension of the user account tied to the project.

Therefore, it is recommended to self-host the project or receive prior consent from the web hosting provider to prevent similar incidents from occurring during the user testing process.

5.3 Future Work

While the initial proof-of-concept for ARPA has demonstrated promising potential for realising a truly passwordless future, further development and testing are crucial for its real-world deployment. This chapter outlines the key areas of focus for future work, aimed at iteratively refining the prototype steered by user feedback and ultimately facilitating its transition into a robust and secure solution for broader adoption.

It will therefore be focusing on improving the usability and effectiveness of the ARPA scheme in the coming days by addressing specific usability concerns, enhancing the overall user experience, and ensuring the scheme's resilience against various attack vectors. In addition to building upon the valuable insights gleaned from the initial user testing with close-ended surveys, the next (planned) endeavours are going to be as follows:

- Work towards incorporating the points raised in the recommendations section of this thesis to pave the way for a more secure and user-friendly experience for everyone in future iterations of the scheme.
- Prepare a comprehensive report summarising the experiment design, results, and insights for future iterations of the ARPA scheme.
- Measure the average login and session resumption times during a load test with hundreds, if not thousands, of (simulated) users simultaneously trying to access their accounts at peak hours.

- Measure system performance metrics by reviewing the aRBA risk engine logs to calculate the false positive and false negative rates to assess the accuracy of the scheme. This is vital for measuring ARPA's ability to differentiate between legitimate and fraudulent login attempts.
- Measure the memory and CPU usage during authentication processes, particularly during a load test with a large but realistic number of users. Evaluate system resource utilisation to gauge the scalability and performance of the ARPA prototype.
- Give users the ability to adjust their level of security:
 - **Low-security mode:** Offers the quickest and easiest login experience, but with the least protection. It is ideal for frequent low-risk situations or trusted devices where speed and ease of access are paramount. It stands to save the most amount of time by potentially offering instant logins due to a more relaxed risk assessment. It would also allow users to opt out of certain types of data being logged about them for use by the aRBA component.
 - **Medium-security mode (default):** Offers a balanced risk assessment and adapting authentication and re-authentication requests based on context. It is suitable for everyday use, balancing security with ease of access by offering a relatively quick and seamless login experience while also adding an extra layer of security compared to low-security mode.
 - **High-security mode:** Offers a more aggressive risk assessment, thereby prioritising security over speed, time, and convenience if a user's account has a higher risk of being targeted by attackers due to their popularity or assigned roles and privileges. It is also recommended for accessing highly sensitive information or accounts in various high-risk situations.

Future iterations could even allow users to personalise their security levels beyond the three aforementioned preset modes, thereby tailoring protection to specific needs with more granular customisation.

- Future attempts at user testing may include asking volunteers to provide feedback on the ARPA scheme through participating in a think-aloud protocol while using a test build of the scheme and then engaging in a semi-structured interview after the experiment. Combined with the closed-ended survey questions, this multi-faceted approach would help capture both quantitative and qualitative data on users' opinions, experiences, and suggestions for further improvement.
- Identify potential areas for improvement in future development of the scheme based on user feedback and data analysis from further testing. This will greatly improve finding as well as addressing previously unknown edge cases with the help of a larger sample size of volunteers.
- Develop a modular architecture that allows ARPA to be easily integrated with a variety of different technology stacks and userbase sizes. This would also allow the integration of the proposed scheme into existing (legacy) systems, thereby making it more easily adoptable.
- Look into the possibility for allowing delegated access and account sharing, all while maintaining robust security.
 - **Delegated Access:** Leverage FIDO2's ability to generate unique credentials for different purposes. This means a user could grant limited access to specific accounts using a dedicated FIDO2 key or biometric, separate from their primary login credentials. The adaptive risk engine component of the ARPA scheme would then continuously assess the legitimacy of delegated access attempts based on the same factors and the account holder's pre-defined security parameters.

- **Account Sharing:** Enable secure account sharing through temporary access codes generated by the ARPA scheme. These codes would be time-sensitive and tied to specific actions, limiting the scope and duration of shared access. Both users could also authenticate with their respective FIDO2 credentials, which would be subject to constant risk assessment.
- The ARPA scheme’s potential to leverage proximity-based authentication via Bluetooth and/or shared WiFi networks for seamless logins is something that warrants further research as it would allow users to quickly and effortlessly authenticate themselves without having to insert their security key or enter their biometric information as simply having a trusted (paired) device or key in close proximity would be more than enough. This could be used in tandem with low and medium-security modes mentioned earlier.
- Further research could be performed to explore how push notifications could be sent out to users’ trusted devices with location-tracking and close proximity detection enabled using Bluetooth and shared WiFi networks. This could be a challenge as the ARPA scheme does not currently require the user to install any additional application on their devices for the sake of better adoption and scalability.
- Explore the feasibility of using combining machine learning with behavioural biometrics for the continuous monitoring of actions performed and behaviours presented during an active user session. This could be a possible addition to the aforementioned high-security mode as it can be very intrusive for privacy-conscious users. It can act as a fail-safe measure in the event that an unauthorised person gets a hold of the user’s trusted device or registered authenticator.

- Further research is required for more viable account recovery options in the event that both the primary and fallback authentication methods fail for a user. For instance, if an authenticator or trusted device is lost or stolen, then it can potentially jeopardise the user account tied to that device. Therefore, there needs to be a way to manually revoke trusted devices and FIDO2 authenticators if ever necessary.

Moreover, it is also crucial for users to be able to add multiple FIDO2 authenticators and fallback authentication methods if they desire to have a variety of choices to log in. Future iterations of the ARPA prototype will have the fallback authentication methods that were previously excluded due to time constraints.

- While the ARPA scheme's current design mainly prioritises user security and convenience, improving its overall speed and scalability is also something that warrants further research to accommodate a growing userbase without significant performance degradation.

One potential avenue of interest is exploring the feasibility of incorporating hash tables into specific aspects of the scheme's architecture as they offer a significant speed advantage for searching large datasets due to their ability to directly access data based on calculated hash values, making them very suitable for fast data retrieval.

A fast and secure hashing algorithm could be used prior to storing frequently accessed user data and risk assessment parameters, thereby reducing lookup times and leading to improved response times, quicker risk score calculation, and resilience against denial of service attacks. However, it may lead to increased memory and CPU usage as well.

- Explore the possibility for balancing privacy and security by utilising alternative approaches like RTT instead of logging users' IP addresses for the geolocation and geo-velocity factors used by the risk assessment engine component of the proposed ARPA scheme.

Unlike IP addresses, RTT does not directly reveal the user's physical location. Instead, it is a measurement of the network latency between a user's device and the server. This enhances user privacy by reducing the amount of personal data collected and stored by the system.

Further research and analysis are needed to determine the effectiveness of RTT in accurately distinguishing between users in similar network environments like being in the same room or building due to being co-workers, neighbours, or classmates.

It can potentially be a feature for users who opted out of having their IP addresses being logged by the scheme and have chosen low and medium-security mode. It may also be capable of thwarting geolocation and IP address spoofing as attackers would require physical access to the user's device or network environment instead of simply using a VPN connection.

- While FIDO2 offers significant security advantages over traditional password-based authentication, it is not entirely immune to vulnerabilities. Recent research, particularly a paper published in late 2023, has identified potential attack vectors involving malware that can compromise FIDO2 deployments using malicious browser extensions among other vectors. Therefore, there is a compelling need for investigating and developing strategies to mitigate potential malware-based attacks on FIDO2 re-authentication mechanisms.

- A comprehensive security analysis should be conducted to identify and evaluate potential security vulnerabilities in the proposed ARPA scheme. The analysis must focus on assessing the resilience of the proposed user authentication scheme against common as well as more newer attack vectors.
- Making the ARPA scheme's codebase open source on platforms like GitHub presents a compelling opportunity to massively accelerate its development and adoption as it allows for collaboration with experts and volunteers, community contributions, better transparency, and of course, faster development to realise a truly passwordless future.

The above-mentioned points provide a detailed scope of work for not only identifying potential limitations within the current study, but it also defines numerous areas for improvement in the proposed ARPA scheme's future design and implementation.

By addressing these key areas of future work, the scheme's design can be massively overhauled for transforming it from a promising concept into a robust, practical, and widely deployable passwordless user authentication solution that is inherently 2FA/MFA and offers enhanced user security, convenience, and privacy in real-world applications.

References

- Alam, A., Krombholz, K., & Bugiel, S. (2019). Poster: Let history not repeat itself (this time) – tackling webauthn developer issues early on. In *Proceedings of the 2019 acm sigsac conference on computer and communications security* (p. 2669–2671). New York, NY, USA: Association for Computing Machinery. Retrieved from <https://doi.org/10.1145/3319535.3363283> doi: 10.1145/3319535.3363283
- Alappat, M. R. (2023). *Multifactor authentication using zero trust* (Unpublished doctoral dissertation). Rochester Institute of Technology.
- Al Kabir, M. A., & Elmedany, W. (2022, December). An overview of the present and future of user authentication. In *2022 4th ieee middle east and north africa communications conference (menacomm)* (pp. 10–17). IEEE. doi: 10.1109/MENACOMM57252.2022.9998304
- Alqubaisi, F., Wazan, A. S., Ahmad, L., & Chadwick, D. W. (2020). Should we rush to implement password-less single factor fido2 based authentication? In *2020 12th annual undergraduate research conference on applied computing (urc)* (pp. 1–6).
- Barbosa, M., Boldyreva, A., Chen, S., & Warinschi, B. (2021). Provable security analysis of FIDO2. In *Advances in cryptology – CRYPTO 2021* (pp. 125–156). Cham: Springer International Publishing.
- Bindel, N., Cremers, C., & Zhao, M. (2023, May). FIDO2, CTAP 2.1, and WebAuthn 2: Provable Security and Post-Quantum Instantiation. In *2023 IEEE Symposium on Security and Privacy (SP)* (pp. 1471–1490).

IEEE. doi: 10.1109/SP46215.2023.10179454

- Brendel, J., Clermont, S., & Fischlin, M. (2023). *Post-quantum asynchronous remote key generation for fido2 account recovery*. Cryptology ePrint Archive, Paper 2023/1275. Retrieved from <https://eprint.iacr.org/2023/1275> (<https://eprint.iacr.org/2023/1275>)
- Bursztein, E., & Kaczmarczyk, F. (2023, August). *Toward quantum resilient security keys*. <https://security.googleblog.com/2023/08/toward-quantum-resilient-security-keys.html>. (Accessed: 2023-8-18)
- Farke, F. M., Lorenz, L., Schnitzler, T., Markert, P., & Dürmuth, M. (2020). “you still use the password after all” — exploring FIDO2 security keys in a small company. In *Proceedings of the sixteenth USENIX conference on usable privacy and security* (pp. 19–35). Usenix Association.
- FIDO Alliance. (2021, November). *FIDO authenticator allowed cryptography list*. <https://fidoalliance.org/specs/fido-security-requirements/fido-authenticator-allowed-cryptography-list-v1.4-fd-20211102.html>. (Accessed: 2022-5-26)
- FIDO Alliance. (2022, April). *FIDO alliance member companies & organizations*. <https://fidoalliance.org/members/>. (Accessed: 2022-5-26)
- Freeman, D., Jain, S., Dürmuth, M., Biggio, B., & Giacinto, G. (2016). Who are you? a statistical approach to measuring user authenticity. In *Network and distributed system security symposium* (pp. 856–870). Retrieved from <https://api.semanticscholar.org/CorpusID:17232548>
- Georgiadis, E. (2023). *Fido2 overview, use cases, and security considerations* (Doctoral dissertation, Athens University of Economics and

- Business). doi: 10.13140/RG.2.2.13329.40806
- Ghorbani Lyastani, S., Schilling, M., Neumayr, M., Backes, M., & Bugiel, S. (2020). Is FIDO2 the kingslayer of user authentication? a comparative usability study of FIDO2 passwordless authentication. In *2020 IEEE symposium on security and privacy (SP)* (pp. 268–285). IEEE.
- Hu, K., & Zhang, Z. (2016). Security analysis of an attractive online authentication standard: FIDO UAF protocol. *China Commun.*, 13(12), 189–198.
- Kabir, M. A. A., Elmedany, W., & Sharif, M. S. (2023). Securing iot devices against emerging security threats: Challenges and mitigation techniques. *Journal of Cyber Security Technology*, 7(2), 1–25. doi: 10.1080/23742917.2023.2228053
- Kepkowski, M., Machulak, M., Wood, I., & Kaafar, D. (2023). *Challenges with passwordless fido2 in an enterprise setting: A usability study*.
- Klieme, E., Wilke, J., van Dornick, N., & Meinel, C. (2020). FIDOnuous: A FIDO2/WebAuthn extension to support continuous web authentication. In *2020 IEEE 19th international conference on trust, security and privacy in computing and communications (TrustCom)* (pp. 1857–1867). IEEE.
- Koved, L. (2015). *Usable multi-factor authentication and risk-based authorization* (Tech. Rep.). New York: IBM Corporation: Yorktown Research.
- Kunke, J., Wiefeling, S., Ullmann, M., & Iacono, L. L. (2021). Evaluation of account recovery strategies with FIDO2-based passwordless authentication. *CoRR*, arXiv:2105.12477. Retrieved from <https://arxiv.org/abs/2105.12477>
- Kushwaha, P., Sonkar, H., Altaf, F., & Maity, S. (2021). A brief survey of challenge–response authentication mechanisms. *ICT Analysis and Applications: Proceedings of ICT4SD 2020, Volume 2*, 573–581.

- Lassak, L., Hildebrandt, A., Golla, M., & Ur, B. (2021). “it’s stored, hopefully, on an encrypted server”: Mitigating users’ misconceptions about {fido2} biometric {webauthn}. In *30th USENIX security symposium (USENIX security 21)* (pp. 91–108).
- Liu, J., Liu, R., & Lai, Y. (2022). Risk-based dynamic identity authentication method based on the ucon model. *Security and Communication Networks*, 2022.
- Mašek, V., & Novotný, M. (2022). Versatile hardware framework for elliptic curve cryptography. In *2022 25th international symposium on design and diagnostics of electronic circuits and systems (ddecS)* (pp. 80–83). doi: 10.1109/DDECS54261.2022.9770143
- Owens, K., Anise, O., Krauss, A., & Ur, B. (2021). User perceptions of the usability and security of smartphones as {fido2} roaming authenticators. In *Seventeenth symposium on usable privacy and security (SOUPS 2021)* (pp. 57–76).
- Papaioannou, M., Mantas, G., Essop, A., Cox, P., Otung, I. E., & Rodriguez, J. (2021). Risk-based adaptive user authentication for mobile passenger id devices for land/sea border control. In *2021 IEEE 26th international workshop on computer aided modeling and design of communication links and networks (camad)* (pp. 1–6).
- Papaioannou, M., Pelekoudas-Oikonomou, F., Mantas, G., Serrelis, E., Rodriguez, J., & Fengou, M.-A. (2023). A survey on quantitative risk estimation approaches for secure and usable user authentication on smartphones. *Sensors*, 23(6), 2979.
- Ranise, S., Sciarretta, G., & Tomasi, A. (2020). Enroll, and authentication will follow. In *Foundations and practice of security* (pp. 156–171). Cham: Springer International Publishing.
- Rasmussen, B. (2021). *A usability study of fido2 roaming software tokens as a password replacement* (Unpublished doctoral dissertation).

Brigham Young University.

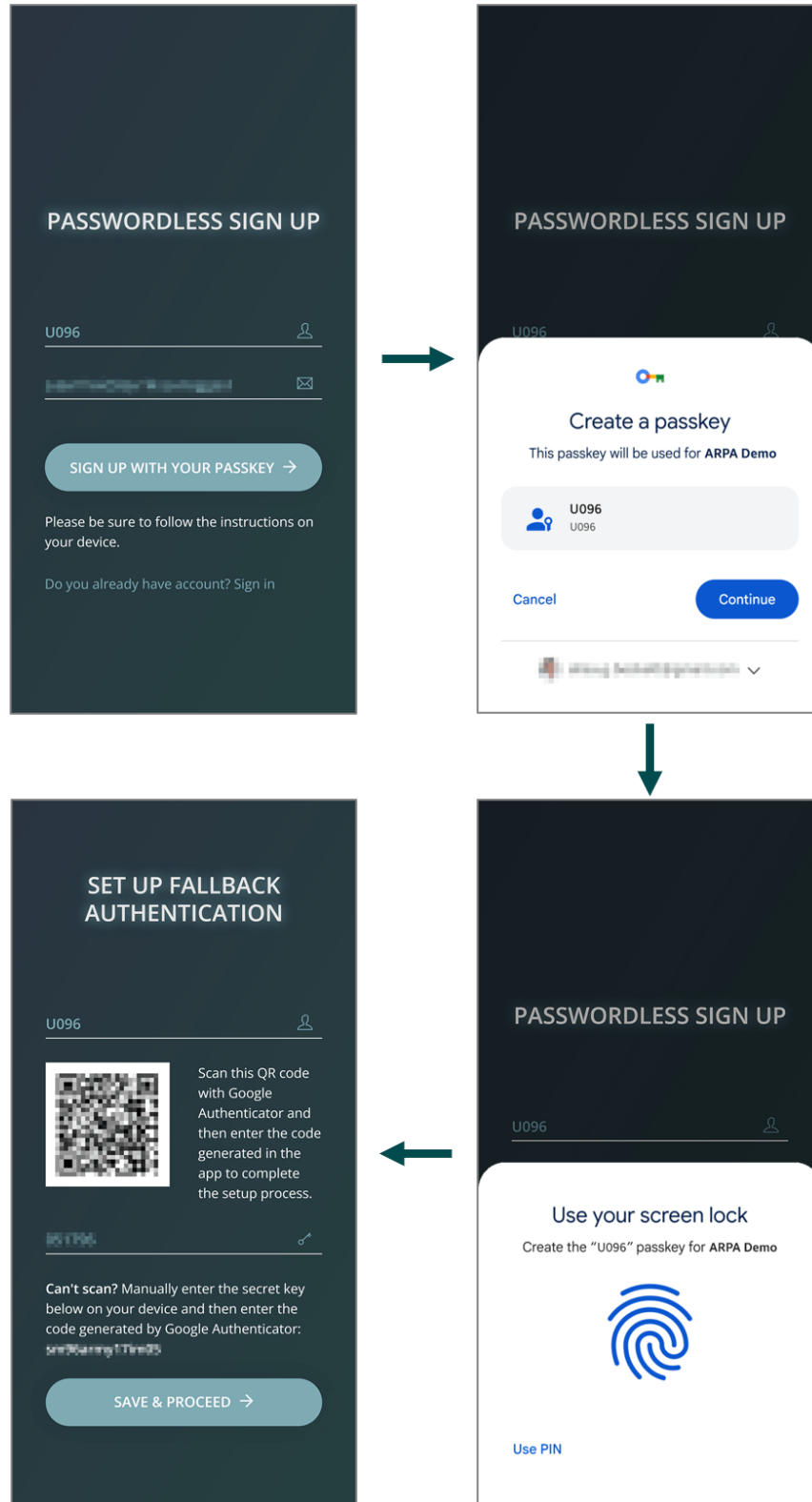
- Rivera, E., Tengana, L., Solano, J., Castelblanco, A., López, C., & Ochoa, M. (2020). Risk-based authentication based on network latency profiling. In *Proceedings of the 13th acm workshop on artificial intelligence and security* (p. 105–115). New York, NY, USA: Association for Computing Machinery. Retrieved from <https://doi.org/10.1145/3411508.3421377> doi: 10.1145/3411508.3421377
- Solano, J., Camacho, L., Correa, A., Deiro, C., Vargas, J., & Ochoa, M. (2021). Combining behavioral biometrics and session context analytics to enhance risk-based static authentication in web applications. *International Journal of Information Security*, 20(2), 181–197.
- Unsel, V., Wiefling, S., Gruschka, N., & Lo Iacono, L. (2023). Risk-based authentication for openstack: A fully functional implementation and guiding example. In *Proceedings of the 13th acm conference on data and application security and privacy* (pp. 237–243).
- Vasileios Grammatopoulos, A., Politis, I., & Xenakis, C. (2021). A web tool for analyzing FIDO2/WebAuthn requests and responses. In *The 16th international conference on availability, reliability and security* (pp. 1–5). New York, NY, USA: ACM.
- Wiefling, S., Dürmuth, M., & Iacono, L. (2020). More than just good passwords? a study on usability and security perceptions of risk-based authentication. In *Annual computer security applications conference* (p. 203–218).
- Wiefling, S., Dürmuth, M., & Iacono, L. (2021). Verify it's you: How users perceive risk-based authentication. *IEEE Security & Privacy*, 19(6), 47–57.
- Wiefling, S., Dürmuth, M., & Lo Iacono, L. (2021). What's in score for website users: A data-driven long-term study on risk-based authentication characteristics. In *Financial cryptography and data security*:

25th international conference, fc 2021, virtual event, march 1–5, 2021, revised selected papers, part ii 25 (pp. 361–381).

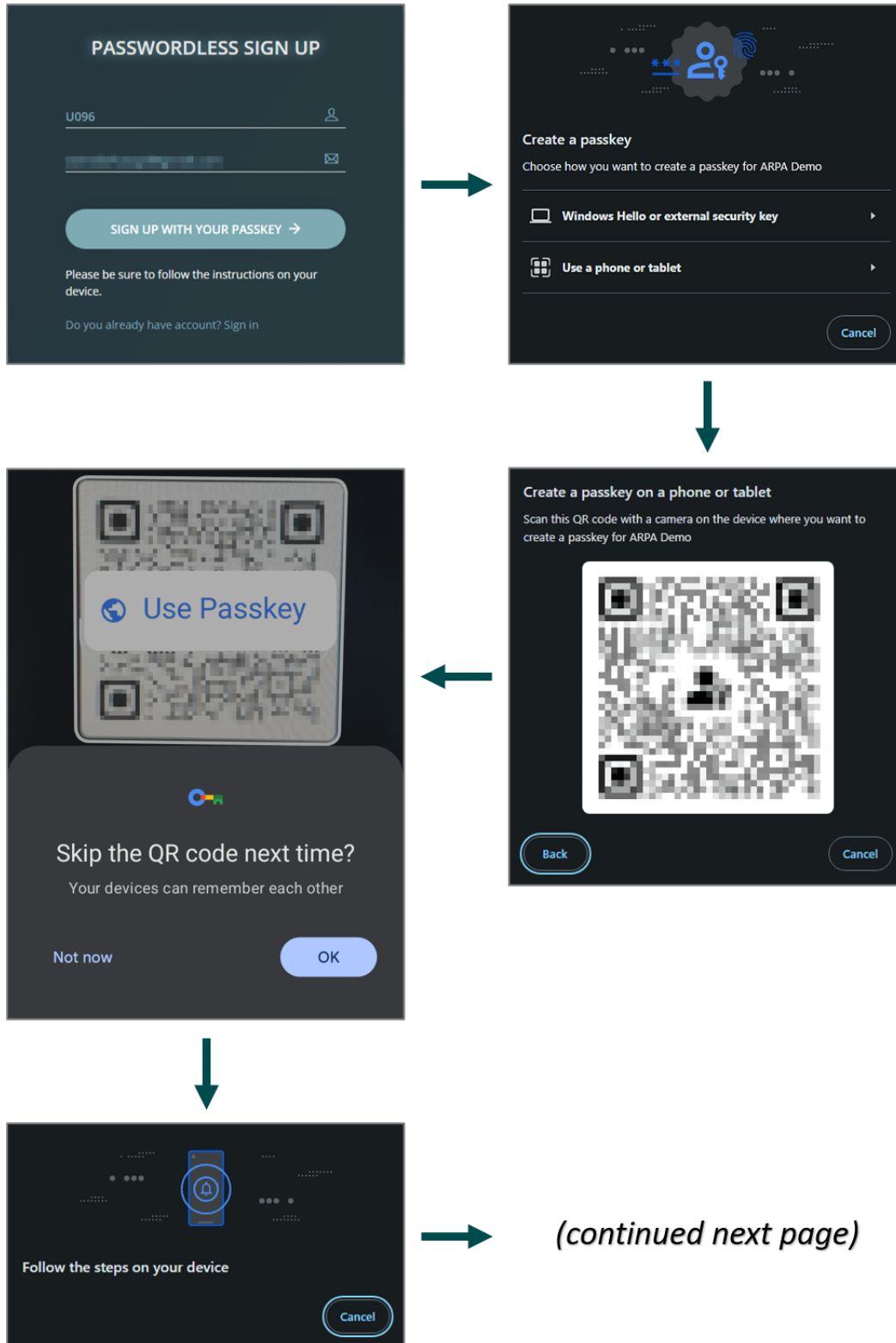
- Wiefling, S., Jørgensen, P. R., Thunem, S., & Iacono, L. L. (2022). Pump up password security! evaluating and enhancing risk-based authentication on a real-world large-scale online service. *ACM Transactions on Privacy and Security*, 26(1), 1–36.
- Wiefling, S., Lo Iacono, L., & Dürmuth, M. (2019). Is this really you? an empirical study on risk-based authentication applied in the wild. In G. Dhillon, F. Karlsson, K. Hedström, & A. Zúquete (Eds.), *Ict systems security and privacy protection* (pp. 134–148). Cham: Springer International Publishing.
- Wiefling, S., Patil, T., Dürmuth, M., & Lo Iacono, L. (2020). Evaluation of risk-based re-authentication methods. In *Ifip international conference on ict systems security and privacy protection* (pp. 280–294).
- Wiefling, S., Tolsdorf, J., & Iacono, L. L. (2021). Privacy considerations for risk-based authentication systems. In *2021 ieee european symposium on security and privacy workshops (euros pw)* (pp. 320–327). doi: 10.1109/EuroSPW54576.2021.00040
- Yamaguchi, R. S., Nakata, T., & Kobayashi, R. (2020). Redefine and organize, 4th authentication factor, behavior. *International Journal of Networking and Computing*, 10(2), 189–199.

APPENDICES

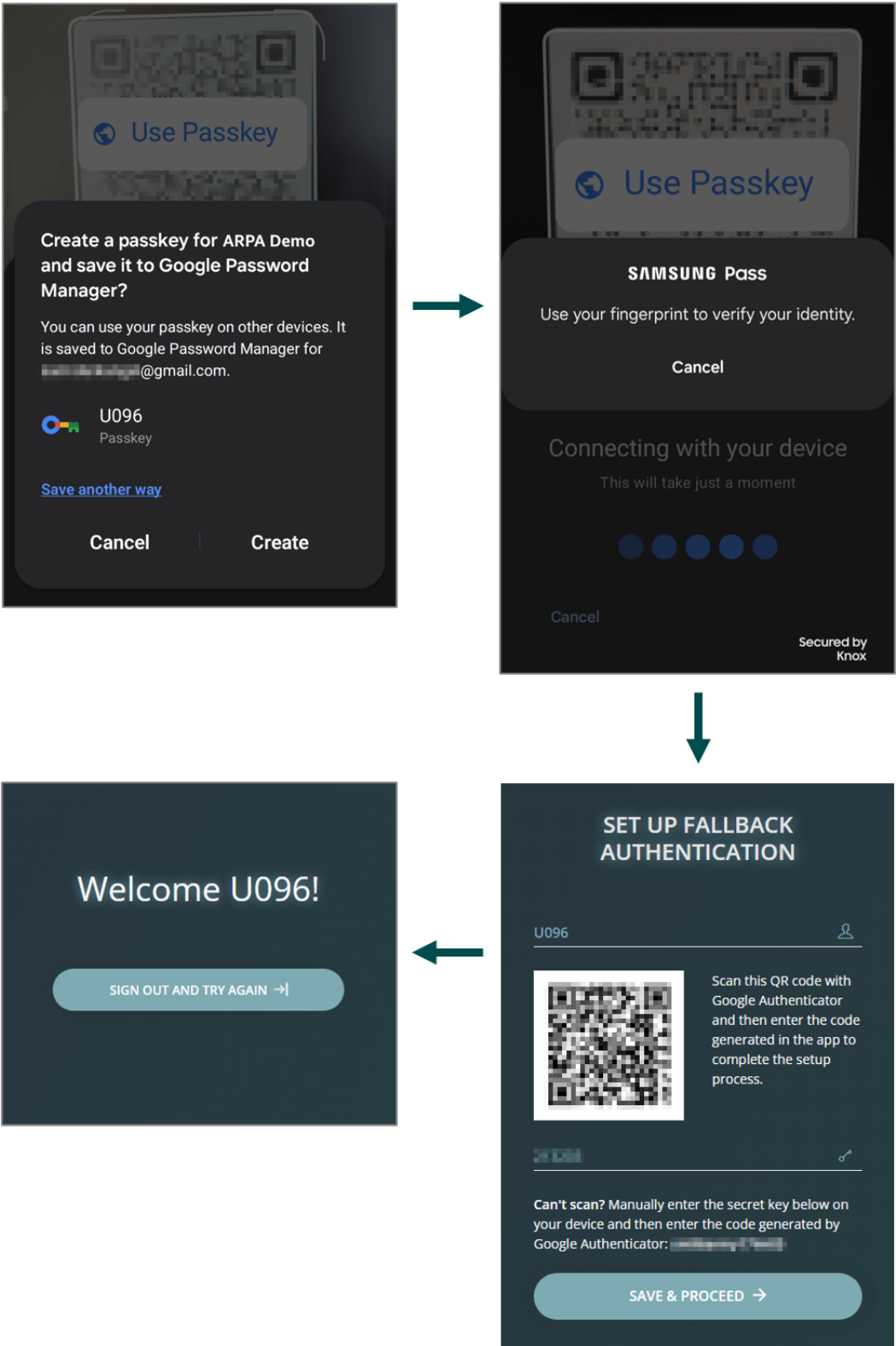
Appendix A: Registration (smartphone as a platform authenticator)



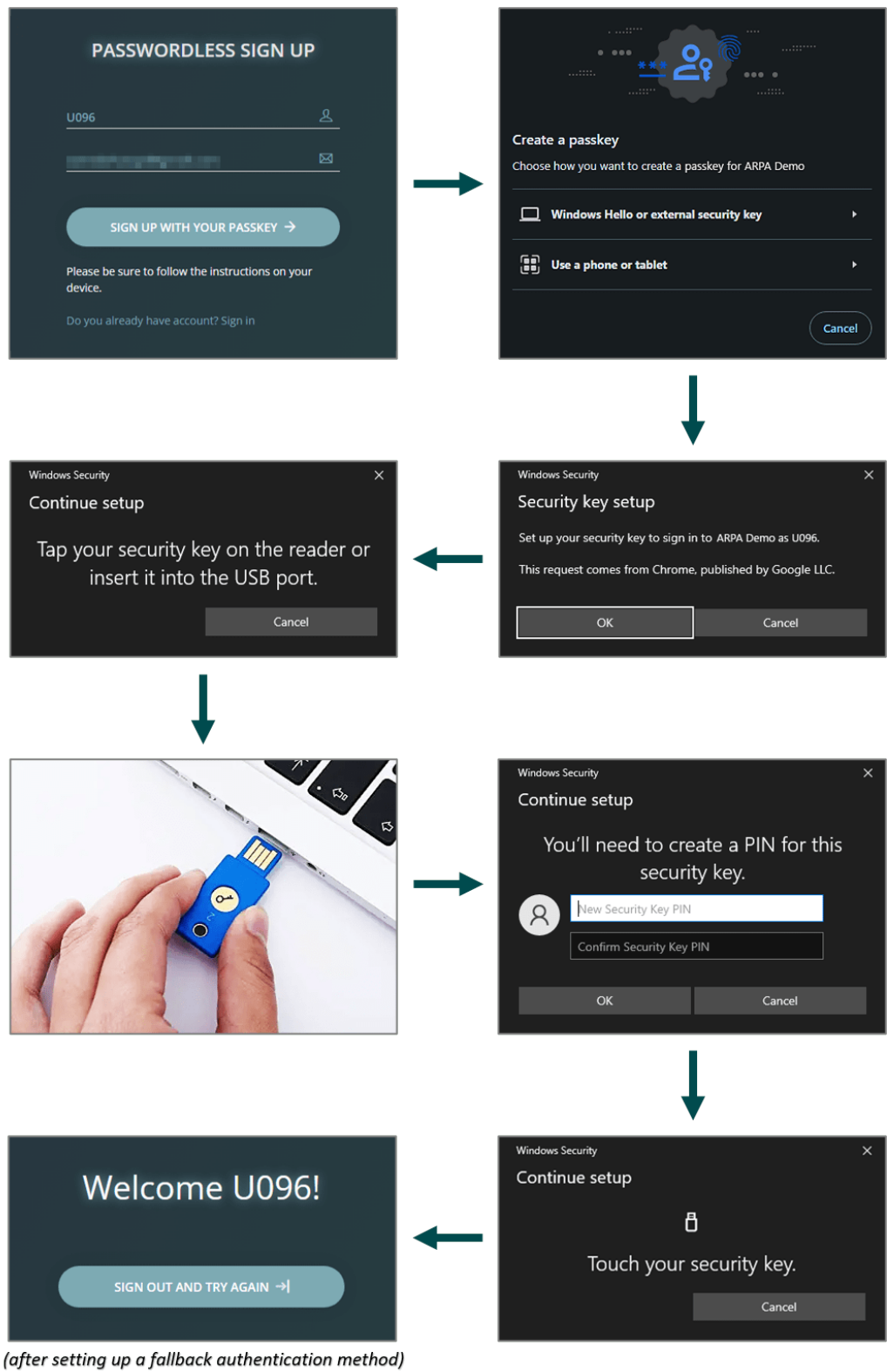
Appendix B: Registration (smartphone as a roaming authenticator)



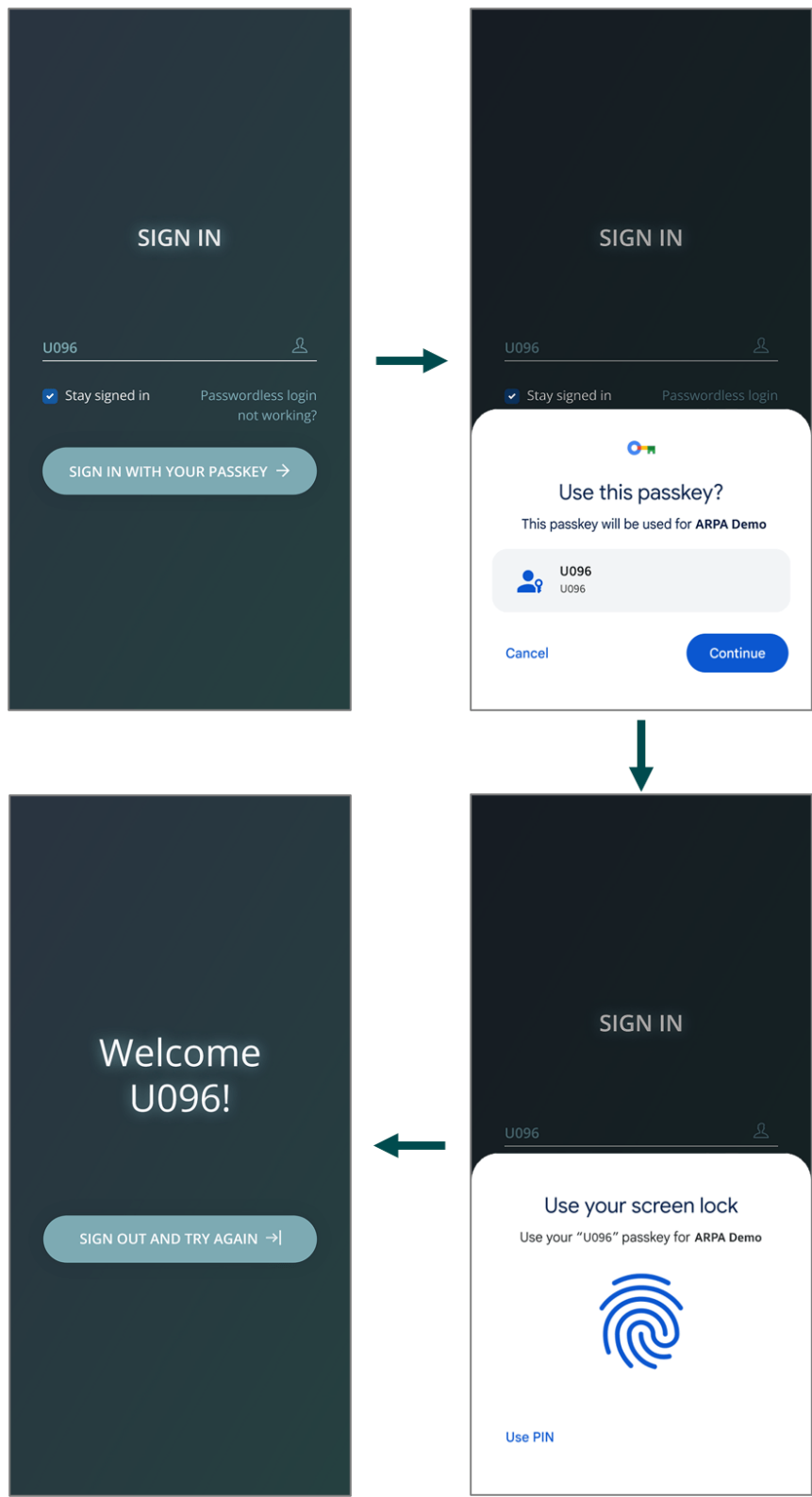
Appendix B: Registration (smartphone as a roaming authenticator) — *continued*



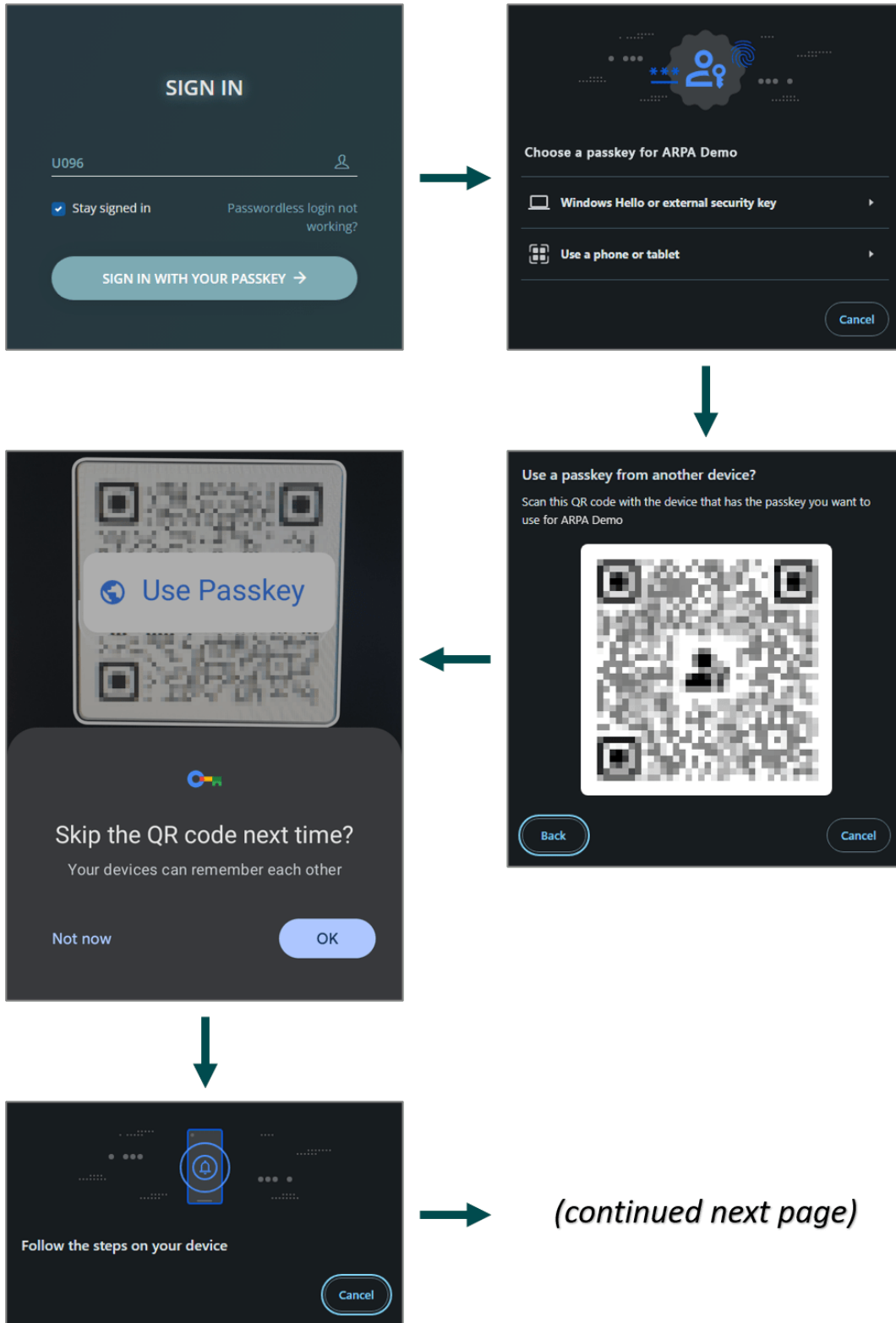
Appendix C: Registration (inserting security key in laptop)



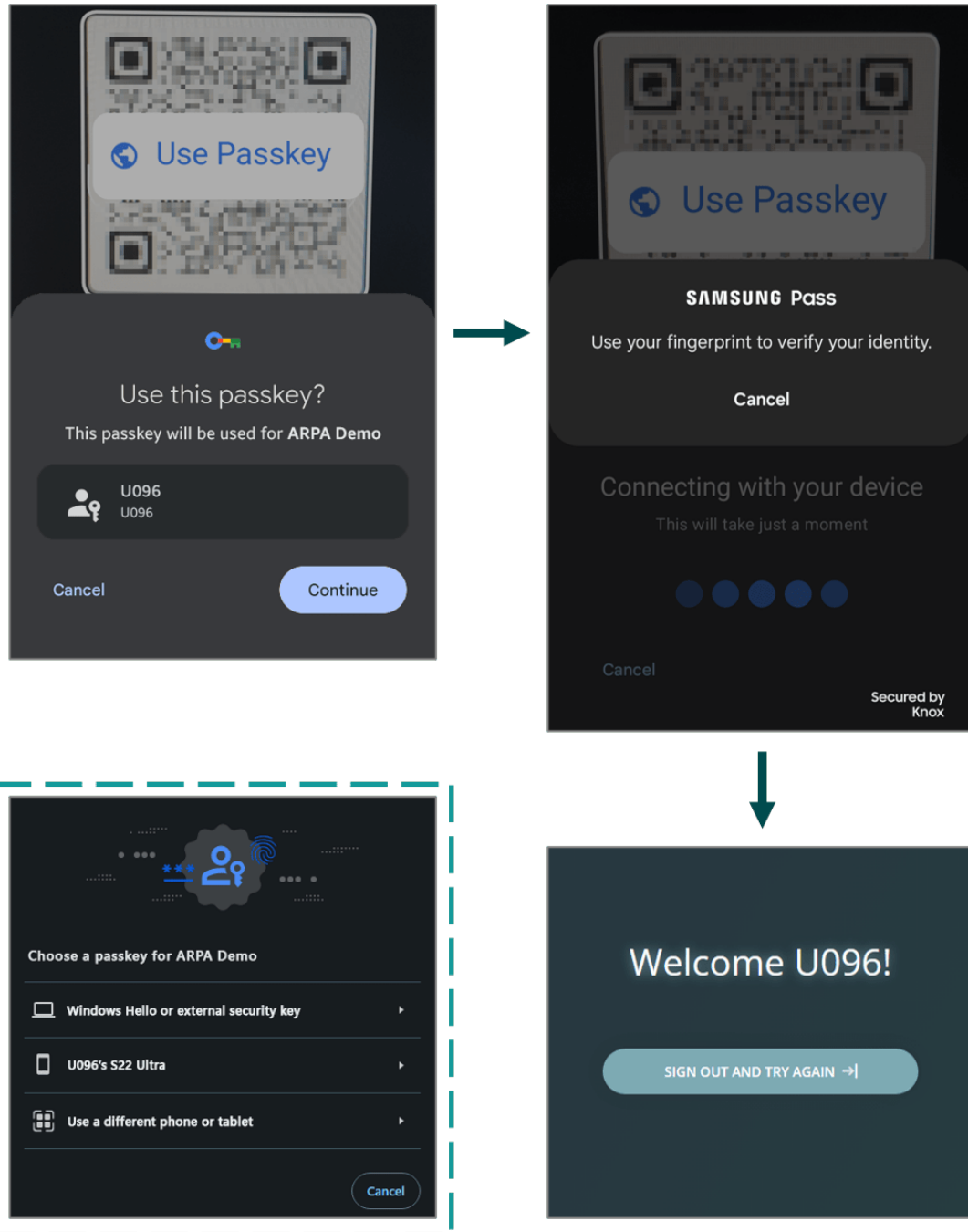
Appendix D: Login (smartphone as a platform authenticator)



Appendix E: Login (smartphone as a roaming authenticator)

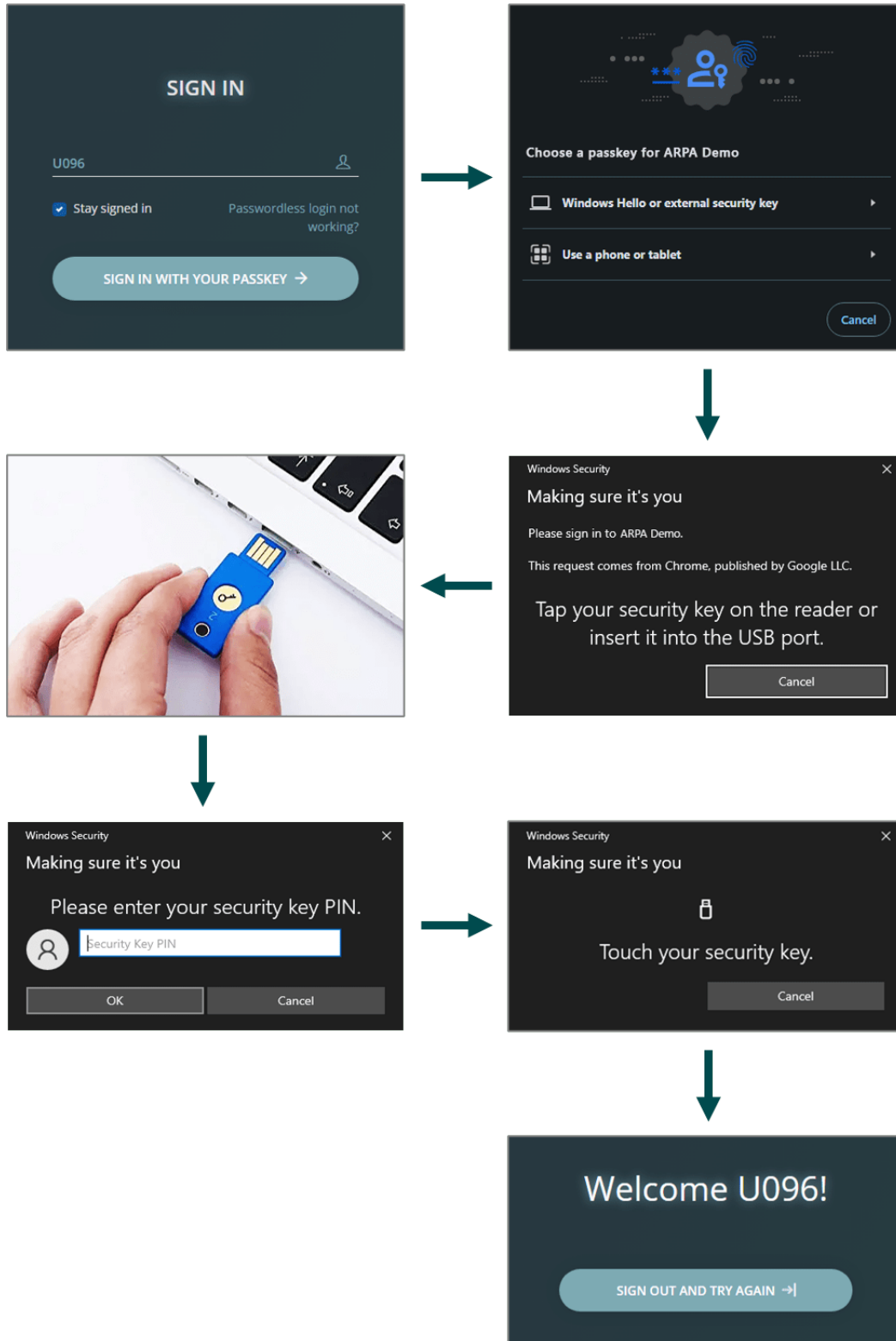


Appendix E: Login (smartphone as a roaming authenticator) — *continued*

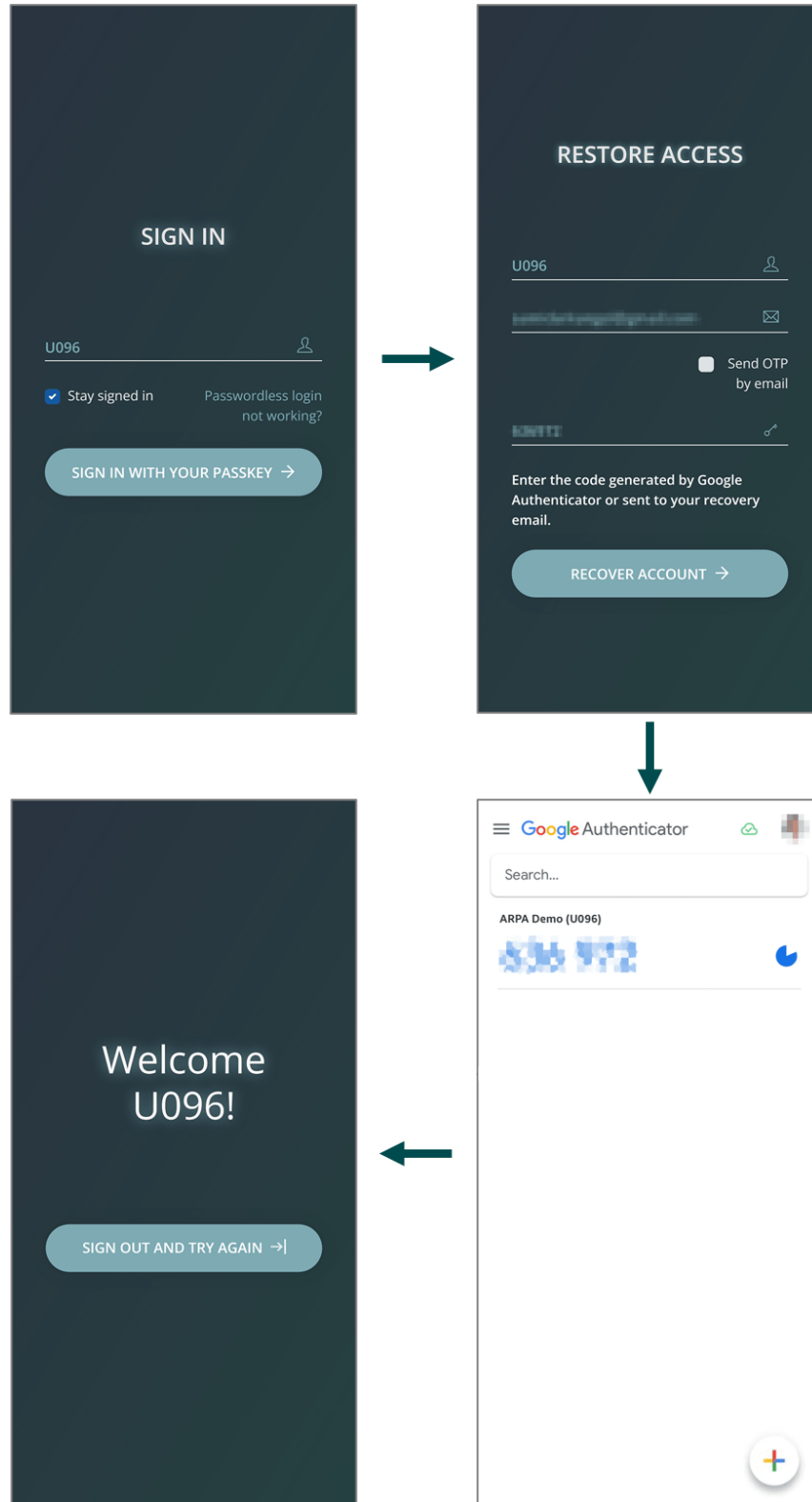


Moving forward, the user (U096) will have the choice to directly choose their saved smartphone and enter their biometric information without having to scan a QR code. This will help them save time in subsequent passwordless logins.

Appendix F: Login (inserting security key in laptop)



Appendix G: Fallback authentication method (Google Authenticator)



Appendix H: Fallback authentication method (OTP via email)

RESTORE ACCESS

U096

☒ Send OTP by email

Enter the code generated by Google Authenticator or sent to your recovery email.

RECOVER ACCOUNT →

Welcome U096!

SIGN OUT AND TRY AGAIN →



is your ARPA account recovery code

Gmail/Inbox

From:

To:

Hi U096,

We're sorry that your passkey isn't working!
Don't worry. You can enter the code below to regain access to your account in no time.

This message was sent to
To help keep your account secure, please don't forward this email. [Learn more](#)

ملخص الدراسة

لطالما كانت كلمات المرور غير آمنة بطبيعتها، ولكن استمرار استخدامها وطبيعتها الشاملة تثير مخاوف أمنية كبيرة في المشهد الرقمي المتطور باستمرار في عصرنا الحالي. يسعى هذا المسعى الأكاديمي إلى استكشاف جدوى مخطط جديد للمصادقة بدون كلمة مرور يعتمد على المخاطر والتكليف (ARPA) يجمع بين نقاط قوة مصادقة FIDO2 والمصادقة التكيفية القائمة على المخاطر. يهدف ARPA إلى معالجة الحاجة المتزايدة لحل قوي وآمن وسهل الاستخدام للمصادقة بدون كلمة مرور من خلال الاستفادة من بروتوكولات المصادقة الآمنة لـ FIDO2 وضبط إجراءات الأمان بشكل ديناميكي بناءً على تحليل المخاطر في الوقت الفعلي. تكمن الفكرة في السماح للمستخدم المقصود بالوصول إلى حسابه بأقل قدر من الإعاقة، بينما يتم تحدي المستخدم الاحتيالي بشكل أكبر أو منعه تمامًا من الوصول لردعه عن مواصلة أجهزته الخبيثة. في حالة اكتشاف مخاطر غير ضئيلة ولكن ليست عالية بما فيه الكفاية، سيُطلب من المستخدمين إعادة المصادقة على أنفسهم باستخدام عامل قائم على السمات البيومترية أو الاستحواذ.

تقدم هذه الأطروحة المنطق التصميمي وراء مخطط ARPA من خلال التركيز على التحديات والفرص المتاحة لتنفيذ مثل هذا المخطط، ولا سيما اعتباراته التقنية والعملية بالإضافة إلى فوائده الملموسة والقيود المحتملة في التطبيقات الواقعية. لتقييم الجدوى العملية، تم تطوير واختبار إصدار إثبات المفهوم الأساسي للمخطط مع مجموعة من المتطوعين. قدمت ملاحظات المستخدم والبيانات التي تم جمعها من خلال أسئلة استطلاع مغلقة رؤى قيمة حول قابلية الاستخدام الملحوظة والأمان وفعالية مخطط المصادقة على المستخدم المقترح.

تُظهر النتائج الواردة هنا حلاً واعداً للمصادقة بدون كلمة مرور. إن الطبيعة المتأصلة لـ 2FA / MFA للمخطط، إلى جانب قدرات تقييم المخاطر التكيفية التي تضبط إجراءات الأمان بشكل ديناميكي بناءً على سلوك المستخدم في الوقت الفعلي والعوامل السياقية، تقدم نهجاً مقنعاً لتعزيز الأمان والخصوصية دون المساومة على راحة المستخدم حيث يمكنهم ببساطة استخدام طريقة تسجيل الدخول المفضلة القائمة على البيانات الحيوية أو الاستحواذ للوصول إلى موقع الويب المفضل لديهم دون الحاجة إلى القلق بشأن عمليات الاستيلاء على الحساب أو تسريبات كلمات المرور أو سرقتها واختراقات البيانات. لدى المستخدمين خيار استخدام مصادقات النظام الأساسي أو المصادقات الخارجية (تجوال) لتسجيل الدخول، وكلاهما يمكن أن يكون بسهولة الهاتف الذكي في جيبهم دون الحاجة إلى تثبيت أي تطبيق إضافي.

تختتم الورقة بتحديد نطاق شامل للعمل المستقبلي، بما في ذلك مزيد من تحسين النموذج الأولي، والاختبار على نطاق واسع، والاندماج مع بيانات العالم الحقيقي. تمهد هذه الأطروحة الطريق لمزيد من الاستكشاف لـ ARPA كبديل قابل للتطبيق وآمن ومتمحور حول المستخدم لأساليب المصادقة التقليدية المعتمدة على كلمة المرور والتي تناسب المؤسسات من جميع الأحجام.

جامعة البحرين

كلية تقنية المعلومات



قسم هندسة الحاسوب

حلاً سريعاً ومتكيفاً للمصادقة متعددة العوامل بدون كلمة مرور

درجة الماجستير في العلوم في الأمن الإلكتروني أطروحة مقدمة كجزء من متطلبات الحصول على

مقدم من

محمد عزيز الكبير

٢٠٢١٠١٢٦٨

يشرف عليها

د. وائل المدني

(أستاذ مشارك)

جامعة البحرين

مايو ٢٠٢٤

مملكة البحرين