

Adaptive Digital Identity Verification Reference Architecture (ADIVRA) Framework

by Memoona Javeria Anwar

Thesis submitted in fulfilment of the requirements for
the degree of

**Doctor of Philosophy (C02029)
Information Systems**

under the supervision of:

Dr Asif Q. Gill

Dr Farookh Hussain

Dr Ghassan Beydoun

University of Technology Sydney
Faculty of Engineering and Information Technology
School of Computer Science
July 2021

Certificate of Authorship

I, Memoona Javeria Anwar, declare that this thesis is submitted in fulfilment of the requirements for the award of Doctor of Philosophy in Information Systems in the Faculty of Engineering and IT, School of Computer Science at the University of Technology Sydney.

This thesis is wholly my own work unless otherwise referenced or acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis. This document has not been submitted for qualifications at any other academic institution.

This research is supported by the Australian Government Research Training Program.

Signature: Production Note:
 Signature removed prior to publication.

Date: 06-07-2021

Acknowledgments

I have been privileged to have Dr Asif Gill, Dr Ghassan Beydoun and Dr Farookh Hussain as my supervisors. I want to express my sincere gratitude to my principal supervisor, Dr Asif Gill, for giving me the opportunity to work with him on this research project. His highly valuable support, coaching, encouragement, quick feedback, and guidance helped me finish this research project. Dr Asif Gill was always there to provide support in meetings, phone conferences, and by email. His valuable understanding in the field of information security, privacy, and digital ecosystems as an academic, researcher, and practitioner provided a wealth of knowledge that I used in this research project.

This study would not have been possible without the support of my family. I am very grateful to my parents, Hameeda Begum (late) and Muhammad Anwar Sheikh (late), for their precious love, blessings, support, encouragement, sacrifice, and care since my childhood. I am thankful for the support of my husband, my children, and siblings. Their genuine care gave me confidence and peace of mind during my busy life. I am blessed to be a member of such a loving, caring, and supportive family.

I want to express my sincere thanks to all my colleagues and friends for their valuable feedback and support.

I also wish to thank the Australian Government for its support for providing the funding for my research project for the length of my PhD study period.

I am thankful to all of the reviewers for their valuable feedback and comments.
Thank you all.

Research Contributions and Publications

During this PhD research project, I collaborated with my supervisor and other colleagues. I published the components of this research work (ADIVRA) in several rigorously reviewed international conference papers and scientific journals. The publication of these papers was an opportunity to present my work for review before including it in this thesis. Appendix F presents a list of the publications that have been included in this thesis.

Publication	Status	Reference	Source
Publication-1	Published	Anwar, M., Gill, A., and Beydoun, G. 2018. "A review of information privacy laws and standards for secure digital ecosystems", in ACIS, 2018, Sydney, Australia.	http://www.acis2018.org/wp-content/uploads/2018/11/ACIS2018_paper_78.pdf
Publication-2	Published	M. J. Anwar and A. Q. Gill, "A Review of the Seven Modelling Approaches for Digital Ecosystem Architecture," 2019 IEEE 21st Conference on Business Informatics (CBI), Moscow, Russia, 2019, pp. 94-103, doi: 10.1109/CBI.2019.00018.	https://ieeexplore.ieee.org/document/8807801
Publication-3	Published	M. Anwar, A. Gill, and G. Beydoun, "Using Adaptive Enterprise Architecture Frame-work for Defining the Adaptable Identity Ecosystem Architecture," 2019.	https://acis2019.io/pdfs/ACIS2019_PaperFIN_176.pdf
Publication-4	Published	M. Anwar and A. Gill, "Developing an Integrated ISO 27701 and GDPR based Information Privacy Compliance Requirements Model," 2020.	https://www.datazoo.com/wp-content/uploads/ISO27701-and-GDPR-Gaps-and-Overlaps.pdf
Publication-5	Published	Secure Big Data Ecosystem Architecture: Challenges and Solutions	https://doi.org/10.1186/s13638-021-01996-2
Publication-6	In Review	A Privacy Assessment Model for GDPR Compliant Blockchain enabled Identity Management: An Action Design Research	Journal of Information and Management
Publication-7	Accepted	PESTLE+ risk analysis model to assess the pandemic preparedness of identity ecosystems	Security and Privacy journal
Publication-8	In Review	Decentralised Digital Identity Requirements Model: Regulatory Perspective	Computer and Security Journal
Publication-9	In Review	Using ArchiMate for Modelling the Secure Digital Identity Ecosystem Architecture	Computer and Security Journal

Table of Contents

Certificate of Authorship	i
Acknowledgments	ii
Research Contributions and Publications	iii
Table of Contents	iv
List of Tables.....	viii
List of Figures	x
List of Abbreviations	xii
<i>Abstract.....</i>	<i>xiii</i>
<i>Chapter 1: Introduction.....</i>	<i>1</i>
1.1. Research Context.....	1
1.1.1. Privacy	2
1.1.2. Personally Identifiable Information (PII)	2
1.1.3. Privacy Principles	3
1.1.4. Digital Identity (DigI)	3
1.1.5. Blockchain.....	4
1.1.6. Regulations	4
1.2. Research Problem.....	5
1.2.1. Research Gaps	6
1.3. Research Question, Aims and Objectives	7
1.4. Significance and Scope.....	9
1.5. Research Contributions and Limitations	11
1.6. Application and Users	11
1.7. Research Strategy	12
1.8. Thesis Outline.....	13
1.9. Summary	14
<i>Chapter 2 Literature Review.....</i>	<i>15</i>
2.1. Conceptual Foundation	15
2.2. Literature Review	16
2.2.1 Digital Ecosystem	16
2.2.2. Privacy.....	19
2.2.3. Personally Identifiable Information (PII)	20
2.2.4. Privacy Challenges reported in (Anwar et al. 2021)	21
2.2.5. Privacy Principles	23
2.2.6. Identity Ecosystem.....	26
2.2.7. Digital Identity.....	27
2.2.9. Models of DigI Verification	29
a) Centralized DigI Verification Model	30
b) Federated DigI Verification Model	30
c) User-Centric DigI Verification Model	31
d) Self-Sovereign/ DDigI Verification Model.....	31

2.2.10. Blockchain	33
2.2.11. DigI Verification	35
2.2.12. Privacy Regulations.....	36
2.2.13. Adaptive Enterprise Architecture.....	37
2.3 Research Gaps and Questions	38
2.4. Research Novelty	39
2.5. Summary	40
<i>Chapter 3: Action Design Research</i>	<i>41</i>
3.1 Background and Context.....	41
3.2. Review of the Research Methods	41
3.2.1. Grounded Theory	41
3.2.2. Case Study	42
3.2.3. Design Science Research.....	42
3.2.4. Action Research.....	42
3.2.5. ADR.....	43
3.2.6. Rationale for choosing ADR.....	43
3.3. ADR Stages	44
3.3.1. Idea formulation.....	46
3.3.2. Problem Formulation.....	47
3.3.3. Build, Intervene and Evaluate.....	48
3.3.4. Reflection and Learning	49
3.3.4.1 ADIVRA Evaluation (BIE, RL)	49
a) Design and Review Workshops.....	50
b) Industry Field Survey.....	50
3.3.5. Formalisation of learning:	52
3.4. Research Ethics.....	53
3.5. Summary	54
<i>Chapter 4: The ADIVRA Framework</i>	<i>55</i>
4.1. The ADIVRA Overview.....	55
4.1.1 ADIVRA Framework Components and Relationships	55
4.1.2. ADIVRA Artefacts and Relationships	56
4.2. Pre-liminary Stage: Understanding the Business Strategy	57
4.3. Assess Component	59
4.3.1 PESTLE+ Model.....	60
4.3.2 Identity Management Privacy Assessment Model (IdMPAM).....	61
4.3.3 Information Security Audit Maturity Model (iSAM2).....	62
4.4. Design Component.....	64
4.4.1. Regulatory Requirements Model (RRM)	64
4.4.2. Compound Digital Identity (CDigI).....	65
4.4.3. Information Security Envelope Architecture (iSEA)	66
4.4.4. Digital Identity Verification Process Model (DigIVPM)	68
a) B2C DigIVPM.....	70
b) B2B DigIVPM.....	70
4.5. Evolve Component.....	73
4.5.1 Digital Identity Verification Adaption Model (DigIVAM)	73

4.6. Summary	75
Chapter 5: Results and discussion.....	76
5.1. The ADVIRA Framework Evolution (alpha to gamma)	76
5.2 BIE & RL Iteration-I (ADIVRA Alpha Version).....	77
5.3 BIE & RL Iteration II (ADIVRA Beta Version)	83
5.4 BIE & RL Iteration III (ADIVRA Gamma Version)	90
5.5 Industry Field Survey	95
a) Survey Planning.....	95
b) Design the Sampling Procedure.....	95
c) Survey Method Selection	97
d) Questionnaire Development	97
e) Collection and Analysis of Data	97
5.5.1 Survey Data Collection	97
a) ADIVRA Individual Components Questionnaire Group Set (Q1 to Q3).....	98
b) ADIVRA Overall Questionnaire Group Set (Q4 to Q8)	99
5.5.2 Survey Data Analysis	99
5.5.2.1 Survey Quantitative Evaluation	99
5.5.2.2 Survey Qualitative Evaluation	108
5.6 Summary	114
Chapter 6: Discussion and Conclusion	115
6.1 ADIVRA Design Principles	115
6.2 Research Implications	118
6.2.1. Implications for Practice.....	118
6.2.2. Implications for Research.....	119
6.3 Key Contributions and Publications	119
6.4 Limitations and Future Work	121
6.5. Conclusion and Summary	123
Bibliography.....	124
Appendices.....	169
Appendix A: Ethical Approval	169
Appendix B: Consent Form.....	171
Appendix C: Survey Invitation Letter.....	174
Appendix D: Online Industry Survey Questionnaire	176
Appendix E: Industry Field Survey Data	180
Appendix F: Research Papers.....	181
Appendix G: Non-Disclosure Agreement.....	182
Appendix H: Feedback Workshops and Meetings	183
Appendix I: Design and Review Workshops comments Log.....	186

Appendix J- Intervention	190
a) Intervention of IdMPAM in IDZ organizational setting.....	190
1. ShoCard.....	190
2. Civic.....	190
3. Evernym.....	191
4. Jumio.....	192
b. Intervention of PESTLE+ model for risk analysis of Coronavirus	195
Case Study	195
c. Intervention of <i>RRM</i>	200
d. Evaluation of DigIVPM Using IdMPAM.....	203
e. Evaluation of <i>CDigI</i>	203
f. Evaluation of <i>iSEA</i>	206
g. Evaluation of <i>DigIVAM</i>	206

List of Tables

Table 1.1 Research Questions, Research Aims and Research Objectives	8
Table 2.1: Research Concepts	15
Table 2.2: Digital Ecosystem (based on Anwar and Gill 2019)	18
Table 2.3 Privacy and Security Challenges of PII identified in (Anwar et al. 2021)	22
Table 2.4: Studies covering Privacy Principles	26
Table 2.5. DigI Verification Model Challenges.....	32
Table 2.6: Blockchain based DigI Solutions.....	34
Table 2.7 Research Gaps.....	38
Table 3.1 Evaluation Criteria.....	45
Table 3.2 Summary of the ADR Process in ADIVRA Development.....	46
Table 3.3 Survey Ratings.....	51
Table 4.1. ADIVRA Components, Artefacts, Input, Output and Kernel Theories	55
Table 4.2. PESTLE+ Macro Environmental Factors	61
Table 4.3. <i>i</i> SAM2 Levels and Requirements	63
Table 4.4. Compound Digital Identity	66
Table 4.5. Decentralized Digital Identity Verification Entities	69
Table 4.6. Digital Identity Verification Adaption Model Activities.....	74
Table 5.1 Assess Component Design and Review Workshop I.....	78
Table 5.2 Assess Component Design and Review Workshop II	80
Table 5.3. <i>i</i> SAM2 Levels and stages	81
Table 5.4 Assess Component Design and Review Workshop III.....	82
Table 5.5 Design Component Design and Review Workshop I	84
Table 5.6 Design Component Design and Review Workshop II.....	88
Table 5.7 Design Component Design and Review Workshop III	89
Table 5.8 Evolve Component Design and Review Workshop I.....	91
Table 5.9 Evolve Component Design and Review Workshop II.....	93
Table 5.10 Evolve Component Design and Review Workshop III.....	94
Table 5.11 Industry Field Survey Participants.....	96
Table 5.12: ADIVRA Assess Component Questions Group	98
Table 5.13: ADIVRA Design Component Questions Group.....	98
Table 5.14: ADIVRA Evolve Component Questions Group.....	98
Table 5.15: Overall ADIVRA Framework Questions Group	99
Table 5.16: Assess Component Survey Rating SR1	100
Table 5.17: Assess Component Category Rating CR1	101
Table 5.18: Design Component Survey Rating SR2	102
Table 5.19: Design Component Category Rating CR2.....	102
Table 5.20: Evolve Component Survey Rating SR3	104
Table 5.21: Evolve Component Category Rating CR3.....	104
Table 5.22: Overall ADIVRA Framework Survey Rating SR4	106
Table 5.23: Overall ADIVRA Framework Category Rating CR4.....	106
Table 5.24: ADIVRA Usefulness Results	109
Table 5.25: ADIVRA Usefulness Ratings (CR5).....	110
Table 5.26: ADIVRA Feedback/Comments and Response	113

Table 5.27: ADIVRA Feedback/Comments Weight Frequency	114
Table 5.28: ADIVRA Framework Overall Rating (CR6).....	114
Table 6.1. Extraction of design principles	115
Table 6.2. Key design principles.....	117
Table 6.3. Publications.....	119

List of Figures

Figure 1.1. Research Gaps	6
Figure 1.2. Research Scope.....	10
Figure 1.3. Adaptive Digital Identity Verification Reference Architecture Framework – High Level Contextual Diagram (reported in Anwar et al. 2021)	11
Figure 1.4. Research Strategy	12
Figure 1.5. Thesis Outline.....	14
Figure 2.1. Conceptual Foundation.....	16
Figure 2.2. Digital Ecosystem adapted from (Gill 2015; Anwar & Gill 2019)	17
Figure 2.3. Privacy Principles.....	20
Figure 2.4. Timeline of Identity management Models	31
Figure 2.5. Digital Identity Verification Entities	35
Figure 3.1 The stages of ADR adapted from Sein et al. (2011), Gill & Chew (2019) and Gregor et al. (2013)	44
Figure 3.2 Idea Formulation	47
Figure 3.3 Problem Formulation.....	48
Figure 3.4 Build, Intervene and Evaluate	49
Figure 3.5 Reflection and Learning	50
Figure 3.6 Formalization of Learning.....	53
Figure 3.6. ADR Methodology	54
Figure 4.1. ADIVRA-Component Artefacts’ relationships	57
Figure 4.2. Strategic Need Analysis Process	57
Figure 4.3. Business Vision and Privacy Goals	58
Figure 4.4. ADIVRA-ASSESS Component	59
Figure 4.5. PESTLE+ Risk Analysis Model.....	60
Figure 4.6. IdMPAM Evaluation Criteria	62
Figure 4.7. ADIVRA-DESIGN Component.....	64
Figure 4.8. Regulatory Requirements Model.....	65
Figure 4.9. Information Security Envelope Architecture.....	68
Figure 4.10. Decentralized Digital Identity Verification Life Cycle	69
Figure 4.11. Digital Identity Verification Process Model.....	72
Figure 4.12. ADIVRA-EVOLVE Component.....	73
Figure 4.13. Digital Identity Verification Adaption Model	74
Figure 5.1. ADIVRA Evolution.....	77
Figure 5.2. BIE & RL Iteration-I	77
Figure 5.3a. PESTLE+ Model (alpha version)	79
Figure 5.3b. IdMPAM Alpha version	79
Figure 5.4. ADIVRA alpha version- High Level Contextual Diagram	82
Figure 5.5. BIE & RL Iteration-II.....	84
Figure 5.6a ADIVRA Design Component (alpha version).....	85
Figure 5.6b Regulatory Requirements Model (alpha version).....	86
Figure 5.6c. Digital Identity Verification Process Model (alpha version)	87
Figure 5.7. ADIVRA beta version- High Level Contextual Diagram	90
Figure 5.8. BIE & RL Iteration-III.....	91
Figure 5.9. Digital Identity Verification Adaption Model (alpha Version).....	92
Figure 5.10. ADIVRA gamma version- High Level Contextual Diagram	94

Figure 5.11. Assess Component Data Graph (BG1)	101
Figure 5.12. Design Component Data Graph (BG2)	103
Figure 5.13. Evolve Component Data Graph (BG3)	105
Figure 5.14. Overall ADIVRA Framework Data Graph (BG4)	107
Figure 5.15. ADIVRA Component Usefulness (BG5)	110
Figure 5.16. Overall ADIVRA Framework Usefulness Rating (BG6).....	112

List of Abbreviations

Abbreviation	Description
ADIVRA	Adaptive Digital Identity Verification Reference Architecture
DigiI	Digital Identity
DDigiI	Decentralized Digital Identity
PII	Personally Identifiable Information
eIDV	Electronic Identity Verification
ADR	Action Design Research
BIE	Build, Intervene and Evaluate
RL	Reflection and Learning
FL	Formalization of Learning
SP	Service Provider
IdP	Identity Provider
IO	Identity Owner
II	Identity Issuer
VC	Verifiable claim
GDPR	General Data Protection Regulation
eIDAS	electronic Identification, Authentication and trust Services
B2B	Business-to-Business
B2C	Business-to-Customer

Abstract

Digital ecosystems comprise interacting actors such as organizations, people and things that are supported by digital platforms. The interconnection of actors may involve sharing personally identifiable information such as digital identity information for verification within the digital ecosystem. One of the key privacy challenges in digital ecosystems is the verification of a digital identity in a manner that is secure and compliant with regulatory requirements. The identity verification process is compromised if personally identifiable information is lost, which can lead to identity theft and more serious instances of data breaches. Therefore, a practical digital identity verification solution should enable secure digital identity verification for actors operating in the inherently complex and diverse regulatory environment of digital ecosystems. Several research and industry initiatives have been taken to address this challenge however, there is a lack of capability in existing solutions and guidance for implementing a digital identity verification solution that can comply to regulatory requirements and securely verify an identity without storing personally identifiable information. Hence, this thesis aims to address a pressing research need: how to ensure regulatory compliance and the privacy of personally identifiable information involved in digital identity verification in a digital ecosystem? This thesis aims to address this practice-oriented research question by proposing an adaptive digital identity verification reference architecture (ADIVRA) framework. The ADIVRA has been incrementally developed by the iterative cycles of build, intervene, and evaluate, reflection and learning, and the formalization of learning research activities following the principles of well-known action design research.

ADIVRA comprises three main components: Assess, Design and Evolve. The Assess component helps to assess the environmental risks and gaps. The Design component fills the gaps identified by Assess component. The third and final component of the ADIVRA framework is Evolve, which analyzes the changes and identifies the adjustments against changing privacy risks, regulatory requirements, and business needs. The proposed ADIVRA framework is evaluated via design and review workshops in industry partners' organizational settings and industry experts' field survey. The results of this evaluation indicate that the proposed ADIVRA framework could be helpful for guiding the development of adaptive digital identity verification solutions that are privacy aware and support regulatory compliance. ADIVRA is intended for use by industry practitioners, law makers, regulators, and researchers as a comprehensive reference architecture for developing privacy aware and regulatory compliant digital identity verification solutions.