UTS UNIVERSITY OF TECHNOLOGY SYDNEY

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

List of Tables

List of Figures

List of Abbreviations

Abbreviation	Description
ADIVRA	Adaptive Digital Identity Verification Reference Architecture
DigI	Digital Identity
DDigI	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.