

An Ontology-Based Identity and Access Management Metamodel for Secure Adaptive Enterprise Architecture

by **Kamrun Nahar**

Thesis submitted in fulfilment of the requirements for
the degree of

Master of Science (Research)

under the supervision of
Associate Professor Asif Qumer Gill
Professor Ghassan Beydoun

University of Technology Sydney
Faculty of Engineering and Information Technology

May 2021

Certificate of Original Authorship

I, Kamrun Nahar, declare that this thesis, is submitted in fulfilment of the requirements for the award of Master of Science (Research) in computing sciences, in the Faculty of Engineering and Information Technology and 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.

Production Note:

Signature: Signature removed prior to publication.

Date:06/05/2021

Acknowledgements

I am thankful to the almighty God for all the grace that I needed to pursue this study. My supervisor Dr Asif Gill and co-supervisor, Dr Ghassan Beydoun, were instrumental in the success of this study. I am grateful for their support and guidance. Their valuable comments, motivation, and enthusiasm kept me inspired and focused. I am incredibly blessed to work with Dr Asif on this research and as a DigiSAS Lab member. His supervision and guidance helped me to achieve my goal. During my research journey, Dr Asif always managed to find time for regular meetings online and in person. His sage advice was instrumental in keeping my research on track.

I would like to thank my parents for their unconditional love, support, prayers and sacrifices for educating me and enabling me to continue this research journey. My deepest gratitude to my husband for his understanding and continuous support which enabled me to complete this research. Without his love and assistance, it would not have been possible for me to continue this journey. I am extremely thankful to my friend Fatema-Tuz-Zohra Khanam for her constant encouragement throughout my research candidature.

I acknowledge my gratitude to the Australian Government Research Training Program for providing the funds and giving me the opportunity to continue my research at the University of Technology Sydney.

List of Publications

1. A Review Towards the Development of Ontology Based Identity and Access Management Metamodel. (Web, Artificial Intelligence and Network Applications Conference, 2020)
Available at: https://doi.org/10.1007/978-3-030-44038-1_21
2. Developing an access control management metamodel for secure digital enterprise architecture modelling. (Security and Privacy Journal, Wiley)
Available at: <http://doi.org/10.1002/spy2.160>
3. Integrated identity and access management metamodel and pattern system for secure enterprise architecture. (Data & Knowledge Engineering, Elsevier) (In Review)

TABLE OF CONTENTS

1.CHAPTER 1: Introduction	1
1.1 Background Context	1
1.2 Research Problem and Question	4
1.3 Research Aim and Objective.....	6
1.4 Research Scope	6
1.5 Research Contribution	7
1.6 Research Strategy.....	10
1.7 Thesis Organisation	11
1.8 Summary.....	12
2.CHAPTER 2: Literature Review	13
2.1 Enterprise Architecture (EA)	14
2.2 Identity Management (IDM) System and Models	16
2.2.1 Isolated Model	19
2.2.2 Centralised Model.....	19
2.2.3 User-Centric Model.....	20
2.2.4 Federated Identity Model.....	20
2.2.4.1 Liberty Alliance	23
2.2.4.2 Shibboleth	24
2.2.4.3 WS-Federation	25
2.3 Access Control Management System and Models.....	25
2.3.1 Mandatory Access Control (MAC) Model	26
2.3.2 Discretionary Access Control (DAC) Model.....	26
2.3.3 Role-Based Access Control (RBAC) Model.....	27
2.3.4 Attribute-Based Access Control (ABAC) Model	29
2.4 Unified Identity and Access Management (IAM).....	30
2.4.1 Conceptual IAM Infrastructure.....	30
2.4.2 Cloud IAM Infrastructure	31
2.4.3 Amazon Web Service (AWS) IAM Infrastructure.....	32
2.5 Conceptual Modelling.....	34
2.5.1 Ontology	35
2.5.3 Model	36
2.5.4 Metamodel	37
2.5.5 Relationships among Model, Metamodel and Ontology.....	38
2.6 Graph Theory	39
2.6.1 Graph Database	40
2.7 Related Work	41
2.7.1 Ontology and Metamodel.....	41
2.7.2 IDM System	42

2.7.3 ACM System.....	43
2.7.4 IAM System.....	45
2.8 Summary.....	47
3.CHAPTER 3: Research Method.....	48
3.1 Design Science Research.....	48
3.2 Applying Design Research Method in Research.....	49
3.2.1 Awareness of Problem.....	49
3.2.2 Suggestion.....	50
3.2.3 Development.....	50
3.2.4 Evaluation.....	51
3.2.5 Outcome.....	52
3.3 Summary.....	52
4.CHAPTER 4: Ontology-based Identity and Access Management Metamodel.....	53
4.1 IAM Metamodel Overview.....	53
4.2 IAM Metamodel Development.....	55
4.2.1 Increment 1: Ontology development for ACM metamodel.....	55
4.2.2 Increment 2: Initial ACM metamodel development.....	58
4.2.3 Increment 3: Final ACM metamodel development.....	60
4.2.4 Increment 4: Ontology development for IDM metamodel.....	62
4.2.5 Increment 5: Initial IDM metamodel development.....	66
4.2.6 Increment 6: Integrated IAM metamodel.....	68
4.3 Summary.....	72
5.CHAPTER 5: Evaluation.....	73
5.1 Patterns for the IAM Metamodel.....	73
5.1.1 Identity Manager Pattern.....	76
5.1.2 Identity Federation Pattern.....	77
5.1.3 Local Authenticator Pattern.....	79
5.1.4 Remote Authenticator Pattern.....	80
5.1.5 Authorisation Pattern.....	83
5.1.6 RBAC Pattern.....	84
5.1.7 Authorisation with Predicate Pattern.....	86
5.1.8 Session Pattern.....	87
5.2 Business Case Study.....	89
5.2.1 Description.....	89
5.2.2 Evaluation.....	90
5.3 Evaluation Results and Insights.....	91
5.4 Summary.....	92
6.CHAPTER 6: Conclusion and Future Research.....	94
6.1 Research Journey.....	94

6.2 Findings.....	94
6.3 Limitations and future research directions.....	96
7.References.....	98

LIST OF FIGURES

Figure 1. 1: Research Contribution Overview	8
Figure 1. 2: IDM and ACM Metamodel Instantiation	8
Figure 1. 3: IAM Metamodel Instantiation	9
Figure 1. 4: IAM Ontology	9
Figure 1. 5: Representation Approach	9
Figure 1. 6: IAM Patterns	10
Figure 1. 7: Research Strategy	10
Figure 1. 8: Research Organisation.....	11
Figure 2. 1: Literature Review Scope	13
Figure 2. 2: Identity Class Diagram (Harry 2013).....	16
Figure 2. 3: Isolated Model (L'Amrani et al. 2016)	19
Figure 2. 4: Centralised Model(Cao & Yang 2010).....	19
Figure 2. 5: User-Centric Model(L'Amrani et al. 2016)	20
Figure 2. 6: Federated Model (Keltoum & Samia 2017)	21
Figure 2. 7: The Circle of Trust (Balasubramaniam et al. 2009).....	21
Figure 2. 8: Elements and Workflow of Liberty Alliance (Fragoso-Rodriguez, Laurent-Maknavicius & Incera-Dieguez 2006).....	23
Figure 2. 9: Elements and Workflow of Shibboleth (Fragoso-Rodriguez, Laurent-Maknavicius & Incera-Dieguez 2006)	24
Figure 2. 10: Elements and Workflow of WS-Federation (Fragoso-Rodriguez, Laurent-Maknavicius & Incera-Dieguez 2006).....	25
Figure 2. 11: MAC Model (Kooker & Kane 2004)	26
Figure 2. 12: DAC Model (Kooker & Kane 2004).....	27
Figure 2. 13: RBAC Model (Kooker & Kane 2004).....	28
Figure 2. 14: (a) Standard RBAC reference models, (b) RBAC ₁ and RBAC ₂ includes RBAC ₀ , where RBAC ₁ adds role hierarchy and RBAC ₂ adds constraints. RBAC ₃ includes RBAC ₁ and RBAC ₂ and by transitivity RBAC ₀ . (Ferraiolo et al. 2001; Sandhu et al. 1996)	28
Figure 2. 15: ABAC Model (Mohamamdi & Kishore 2017).....	30
Figure 2. 16: IAM Functional Infrastructure Schema (MANGIUC 2012)	31
Figure 2. 17: IAM Infrastructure in the Cloud (Yang et al. 2014).....	32
Figure 2. 18: AWS IAM Infrastructure('AWS Identity and Access Management').....	33
Figure 2. 19: Relations between Conceptualisation, Abstraction, Modelling Language and Model (Guizzardi & applications 2007)	35
Figure 2. 20: MDA Four-layer MOF-Based Architecture (Dragan Djurić 2005).....	38
Figure 2. 21: Relationships among the Model, Metamodel and Ontology (Saeki & Kaiya 2006)	38

Figure 3. 1: DSR Steps (Kuechler & Vaishnavi 2011).....	49
Figure 3. 2: Awareness of Problem Phase	50
Figure 3. 3: Suggestion Phase	50
Figure 3. 4: Development Phase	51
Figure 3. 5: Evaluation Phase	51
Figure 3. 6: Outcome Phase	52
Figure 4. 1: Conceptual View of Integrated IAM Metamodel.....	53
Figure 4. 2: ACM Entities and their Relationships.....	58
Figure 4. 3: ACM Metamodel after Increment 2	59
Figure 4. 4: ACM Metamodel after Increment 3	61
Figure 4. 5: IDM Entities and their Relationships	66
Figure 4. 6: IDM Metamodel	67
Figure 4. 7: Entities and their Relationships for Integrating IDM and ACM	69
Figure 4. 8: Integrated IAM Metamodel.....	70
Figure 5. 1: Integrated IAM Pattern System	75
Figure 5. 2: Identity Manager Pattern Metamodel.....	76
Figure 5. 3: Identity Manager Pattern Instance.....	77
Figure 5. 4: Identity Federation Pattern Metamodel	78
Figure 5. 5: Identity Federation Pattern Instance.....	78
Figure 5. 6: Local Authenticator Pattern Metamodel.....	79
Figure 5. 7: Instantiated Local Authenticator Pattern Instance.....	80
Figure 5. 8: Remote Authenticator Pattern Metamodel	81
Figure 5. 9: Instantiated Remote Authenticator Pattern Instance	82
Figure 5. 10: Authorisation Pattern Metamodel.....	83
Figure 5. 11: Instantiated Authorisation Pattern Instance.....	84
Figure 5. 12: RBAC Pattern Metamodel.....	85
Figure 5. 13: Instantiated RBAC Pattern Instance.....	85
Figure 5. 14: Authorisation with Predicate Pattern Metamodel.....	86
Figure 5. 15: Instantiated Authorisation with Predicate Pattern Instance	87
Figure 5. 16: Session Pattern Metamodel	88
Figure 5. 17: Instantiated Session Pattern Instance.....	88
Figure 5. 18: Instantiated Integrated IAM Model for CP.....	91
Figure 6. 1: Research Progress and Plan.....	94

LIST OF TABLES

Table 1. 1: Sub-Questions of RQ.....	5
Table 1. 2: Research Aim.....	6
Table 1. 3: Research Objectives.....	6
Table 1. 4: Research Scope.....	7

Table 2. 1: Security Objectives of Enterprises.....	15
Table 2. 2: IDM Functionalities.....	17
Table 2. 3: Laws of Identity.....	18
Table 2. 4: FIDM Benefits.....	22
Table 2. 5: RBAC Levels.....	29
Table 2. 6: Components of IAM Infrastructure.....	31
Table 2. 7: Cloud IAM Infrastructure Components.....	32
Table 2. 8: Components of AWS IAM Infrastructure.....	33
Table 2. 9: Types of Models Based on Ontological Concepts.....	37
Table 2. 10: Graph Modelling Approach Advantages.....	39
Table 2. 11: The Summary of the Reviewed Related Literature.....	46
Table 3.1: DSR Steps (Kuechler & Vaishnavi 2011).....	48
Table 3.2: Evaluation Criteria.....	52
Table 4. 1. Development Increments.....	55
Table 4. 2: Kernel Theories for ACM.....	56
Table 4. 3: ACM Constructs.....	57
Table 4. 4: ACM Metamodel Entity-Relationship Matrix.....	61
Table 4. 5: Kernel Theories for IDM.....	62
Table 4. 6: IDM Constructs.....	64
Table 4. 7 : IDM Metamodel Entity-Relationship Matrix.....	68
Table 4. 8: Constructs for Integrating IDM and ACM.....	69
Table 5. 1: Elements of the Pattern Template (Gill et al. 2016).....	74
Table 5. 2: Patterns for the IAM Metamodel.....	74
Table 5. 3: Evaluation Result.....	91

Abstract

Security, driven by the need of securing digital assets, is an indispensable component of a modern digital enterprise. An identity and access management (IAM) system is a vital element of secure digital enterprise architecture (EA). IAM is a combination of identity management (IDM) and an access management system (ACM) where IDM ensures secure access to enterprise resources by verifying an entity's identity. On the other hand, ACM grants appropriate access to protected resources. Developing an adaptive IAM system that fulfils business requirements and can grow over time with the continually evolving business environment is challenging. This demands an ontology-based IAM metamodel, which is adaptive and can be instantiated for different situations. Ontologies are useful to unambiguously conceptualise various constructs of a domain and the interrelations among them. On the other hand, a metamodel defines the semantics of a modelling language. It offers a set of elements that can be utilised to create a model. An IAM metamodel that is founded on an IAM ontology can be semantically expressed, communicated, and managed. This IAM metamodel can be used to create a domain-specific IAM model. This research addresses this need and develops an ontology-based integrated IAM metamodel for secure digital EA using the well-known design science research (DSR) method.

The integrated IAM metamodel has four main components: IAM ontology, IDM metamodel, ACM metamodel, and the integrated IAM metamodel. The IAM ontology provides detailed, unambiguous meaning to the necessary IAM-related entities and their relationships. The IDM metamodel offers the set of elements, based on ontology, required to model an IDM system for a particular context. Similarly, the ACM metamodel provides the necessary elements to create domain-specific models for ACM systems. Finally, the integrated IAM metamodel is developed by combining the IDM and ACM metamodels, allowing an enterprise to model their IDM system and ACM system in an integrated manner. The proposed IAM metamodel is evaluated using the demonstration method from DSR. An IAM pattern system has been instantiated using the metamodel for evaluation purposes, consisting of eight patterns. Each pattern focuses on a specific IAM-related problem. Furthermore, a case study has been performed to evaluate the applicability of the developed metamodel. The result of this research indicates that the proposed ontology, metamodel and patterns can be used by academic and architects to

design and implement situation-specific IDM and ACM architectures and solutions within the overall context of a secure digital enterprise architecture.