UTS UNIVERSITY OF TECHNOLOGY SYDNEY

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.

Signature: Production Note:
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

LIST OF FIGURES

LIST OF TABLES

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.