AN ACCESS CONTROL PERSPECTIVE TO SHARING DATA IN A FEDERATION

A THESIS

submitted by

REENA SINGH

for the award of the degree

of

DOCTOR OF PHILOSOPHY

SCHOOL OF COMPUTING AND ELECTRICAL ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY MANDI

OCTOBER 2017

Dedicated to

my father

Late Shri Govind Singh

THESIS CERTIFICATE

This is to certify that the thesis titled **An Access Control Perspective to Sharing Data in a Federation**, submitted by **Reena Singh** to the Indian Institute of Technology, Mandi, for the award of the degree of **Doctor of Philosophy**, is a bonafide record of the research work done by her under my supervision. The contents of this thesis, in full or in parts, have not been submitted to any other institute or university for the award of any degree or diploma.

Date: **Prof. Timothy A. Gonsalves**

Place: Guide

Acknowledgements

I extend my sincerest thanks to my guide Prof. Timothy A. Gonsalves for his advice and guidance throughout my research work. He has taught me how to question thoughts and express ideas. His patience, clarity and decision making skills has helped me at all stages during my work.

I thank the members of my doctoral committee Prof. Deepak Khemani, Prof. B. D. Chaudhary, Dr. Anil Sao, Dr. Varun Dutt and Dr. Manoj Thakur for their constructive feedback during my interactions with them. Their insight and questions were very helpful in streamlining the work.

I thank Dr. Dinil Mon Divakaran for his inputs which helped me get started in the beginning of my research. Special thanks to Dr. Shankar Raman for his helpful suggestions throughout my research. I thank Dr. Astrid Kiehn for the excellent interactions about my work. I sincerely thank Prof. Krishna Sivalingam for his support. I also thank Dr. Yvonne Dittrich, Dr. Ingrid Shockey, Dr. Gaurav Raina, Dr. Ravi Kottada, Prof. Hema Murthy and Dr. Aniruddha Chakraborty for always encouraging me. I thank my seniors Dr. Dileep A. D. and Dr. Veena T. for always being there to listen and give advice to me.

I thank Dr. Priscilla Gonsalves for her motivation and clarity in thinking which helped me in so many ways during my stay here. I am also thankful for her reviews which helped in bringing the thesis to a good shape. I also thank Martin Vestergaard for his reviews and feedback to improve the thesis.

I thank Ministry of Human Resource Development (MHRD)- Govt. of India, for providing me stipend during my PhD. My sincere thanks to Indian Institute

of Technology, Mandi for providing an environment to learn so many things in life throughout the programme. My special thanks to other faculty and staff members of IIT Mandi for providing an encouraging atmosphere all these years. I sincerely acknowledge the help and support of my staff friends who made life here so easy for me, Chandan, Monika, Manoj, Prakash, Nishant and Leeladhar to name a few.

I also thank my teachers Dr. Shrikant Burje and Mr. Mukesh Chauhan who motivated me to pursue research.

I am grateful to my friends for providing support whenever needed, keeping me motivated and giving me numerous moments to cherish in life. I thank Vysakhi, Shivank, Santosh, Shilky, Aparna, Kalyan, Raghavendra, John, Anuradha, Seema, Pradeep, Joginder, Abeba, Neha and Pavin. Thanks to Prashant for the discussions which helped me get clarity in work. Special mention to Suma for consistently keeping me sane throughout this degree and grooming me in so many ways. Also, many thanks to Ritu, Hemant, Anoop, Runa, Sujeet and Anna for their unconditional support.

This journey would not have been possible without the support of my family. They have been a source of motivation throughout. No words are enough to thank them for their incessant support in every facet of my life.

Reena Singh

"It is a great profession. There is the satisfaction of watching a figment of the imagination emerge through the aid of science to a plan on paper. Then it moves to realization in stone or metal or energy. Then it brings jobs and homes to men. Then it elevates the standards of living and adds to the comforts of life. That is the engineer's high privilege."

Herbert Hoover

Abstract

Digital objects such as documents, images, and other media are shared between users belonging to different organisations. A federation refers to one model of interaction of independent organisations for data sharing. It involves each organisation carrying out its local functions independently based on its internal policies, yet respecting federation contracts when it comes to handling data shared by other organisations. Rural Business Process Outsourcing (RBPO), Multi-Institution Course Management System (MI-CMS) and Media Streaming Service (MSS) are some examples of federation.

Data access by users across organisations in a federation takes place over the Internet. In RBPO scenarios, users are geographically distributed throughout the country in cities, towns and villages. In MI-CMS instructors and students belong to different geographically separated organisations and are connected over network. Media is stored on cloud servers in MSS scenarios and accessed by users connecting from different locations over the Internet. In these scenarios network intermittency becomes a serious problem limiting access, affecting the timely access of data by users. The network can become intermittent as the result of a physical link failure or due to administrative policies which may disallow external access during certain periods of time. The last mile access is often through wireless. Thus, the network becomes unavailable many times and even if available, signal strength is mostly low and is shared by many users.

Data provided by an organisation differ in value based on the nature of the application. The patient health-sheet and medical report provided by a health-care organisation has high value. On the other hand, a book outsourced for translation from one language to another has low value. In some applications an object is decomposed into smaller parts before sharing. The value of an individual object gets further reduced by decomposing it into smaller objects. Each of these parts can then be assigned to different users for carrying out different tasks. Once the task is done these parts are composed together. This decomposition allows multiple users to perform tasks in parallel on parts of the same object, thereby

improving the task completion time. Furthermore, since each user has access to only a part of a complete object, the amount of information leakage per user gets reduced.

Shared data is protected from unauthorised access based on the access control policy of the owner organisation. An access control model is a formal representation of the high level access control policy and aids the analysis of security properties exhibited by the access control system. This thesis addresses the security challenges in federations where low value data are shared between users belonging to different organisations in the presence of network intermittency and proposes solutions for the same.

Furthermore, independent organisations participating in a federation have their own terminologies for defining access control policies. When data is shared between organisations a consistent policy needs to be defined which requires understanding and addressing these differences in syntax and semantics.

Towards this objective, first we define a family of access control models called Digital Object Based Access Model (DOBAM) to address the scenarios having a large number of objects and involving object decomposition. We discuss the formalism of DOBAM and verify desirable security properties. Both simulations and analytical models are used to compare the performance of DOBAM with other existing models.

Second, we extend one of the most popular access control models, Role Based Access Control (RBAC) model, to support network-aware access control policies. The resulting model, Network Aware RBAC (NA-RBAC) model, supports specification of access control permissions by taking the network state into account. Restricted access to data can be granted in the temporary absence of network connectivity. We formalise the model and verify different security properties. We compare the performance of NA-RBAC with that of RBAC in the presence of network disconnections. We combine both DOBAM and NA-RBAC to define a family of Network Aware Digital Object Based Access Model (NA-DOBAM) suitable for federation. We formalise the model and verify the security properties.

Third, we also study distributed data access in the presence of permission updates and network disconnections, and we verify the desirable security properties.

Finally, we define NA-DOBAM ontologies for the three federated scenarios, RBPO, MI-CMS and MSS. Access control information is retrieved by querying one or more remote ontologies and access control rules are implemented in the ontology to get new knowledge. We demonstrate these using example scenarios. We show that security constraints and features such as separation of duty and delegation are satisfied by these ontologies.

Contents

Abstract **xi**

List of Figures **xix**

List of Tables **xxi**

Abbreviations **xxiii**

1 Introduction **1**
1.1 Motivation 2
1.1.1 Access Control involving Object Decomposition 3
1.1.2 Sharing Data over Network 4
1.1.3 Ontology for Federation 8
1.2 Objectives and Scope 10
1.3 Contributions 10
1.4 Organisation of the Thesis 12

2 Related Work **13**
2.1 Distributed ACM for Federation 13
2.1.1 Access Control for Object Decomposition 18
2.1.2 Network-Aware Distributed Access Control Model 22
2.2 Access Control Ontology for Federation 24
2.2.1 Semantic Web in Access Control 24
2.2.2 Ontologies for Different Applications 25
2.3 Summary 27

3 Scenarios **29**
3.1 Rural Business Process Outsourcing (RBPO) 31
3.1.1 Nature of Data 33
3.1.2 Data quantity and value 33
3.1.3 Data Generation 33
3.1.4 User Type 34
3.1.5 Level of security 34
3.1.6 Organisations Involved 34
3.1.7 Geographical Spread 34
3.1.8 Sharing Mode 35

3.1.9 Network Availability . . . 35
3.2 Multi-Institution CMS . . . 35
3.2.1 Nature of Data . . . 36
3.2.2 Data Quantity and Value . . . 37
3.2.3 Data Generation . . . 37
3.2.4 User Type . . . 37
3.2.5 Level of Security . . . 37
3.2.6 Organisations Involved . . . 38
3.2.7 Geographical Spread . . . 38
3.2.8 Sharing Mode . . . 38
3.2.9 Network Availability . . . 38
3.3 Media Streaming Service (MSS) . . . 39
3.3.1 Nature of Data . . . 40
3.3.2 Data Quantity and Value . . . 40
3.3.3 Data Generation . . . 40
3.3.4 User Type . . . 41
3.3.5 Level of Security . . . 41
3.3.6 Organisations Involved . . . 41
3.3.7 Geographical Spread . . . 41
3.3.8 Sharing Mode . . . 42
3.3.9 Network Availability . . . 42
3.3.10 Media Caching . . . 42
3.4 Summary . . . 43

4 Digital Object Based Access Model (DOBAM) 45
4.1 DOBAM . . . 46
4.1.1 Core DOBAM . . . 47
4.1.2 Hierarchical DOBAM . . . 50
4.1.3 Conditional DOBAM . . . 51
4.1.4 Administrative Relations in DOBAM . . . 52
4.1.5 Application to RBPO Scenarios . . . 52
4.2 Specification and Verification of DOBAM . . . 55
4.2.1 DOBAM Properties . . . 55
4.2.1.1 Type Correctness . . . 55
4.2.1.2 Safety . . . 56
4.2.1.3 Liveness . . . 56
4.2.2 Model Checking using TLA+ . . . 56
4.2.3 TLA+ Specification . . . 57
4.2.3.1 Type Correctness . . . 57
4.2.3.2 Safety . . . 57
4.2.3.3 Liveness . . . 59
4.2.4 Overview of TLA+ policy Specification and Verification . . . 59
4.3 Comparison with Other Models . . . 61
4.3.1 Comparison of Number of Rules . . . 62

4.3.2 Comparison of the Authorisation Time 64
4.4 Summary 66

5 Network-Aware Access Control Models 69
5.1 Network-Aware RBAC Model 70
5.1.1 Access Authorisation and Permission Management 72
5.1.2 Useful Work Done during Network Disconnection 74
5.2 Formal Specification of NA-RBAC with TLA+ 75
5.2.1 NA-RBAC Properties 75
5.2.1.1 Type Correctness 77
5.2.1.2 Safety 77
5.2.1.3 Liveness 77
5.2.1.4 Consistency 78
5.2.2 Model Checking and Results 78
5.3 Performance Evaluation 79
5.3.1 Analytical Model 80
5.3.2 Simulation and Results 81
5.3.2.1 Effect of Network Disconnection on Access Requests Serviced 82
5.3.2.2 Effect of Network Disconnection on Correct Client Permissions 84
5.3.2.3 Useful work done, HNA-RBAC and RBAC 87
5.4 Network-Aware DOBAM 89
5.4.1 Core NA-DOBAM 90
5.4.2 Hierarchical NA-DOBAM 90
5.4.3 Conditional NA-DOBAM 91
5.4.4 Formal Specification of NA-DOBAM 92
5.5 Summary 95

6 Modelling Distributed Data Access 97
6.1 Scenario for Data Access in a Federation 98
6.2 UPPAAL model 99
6.2.1 Network Template 100
6.2.2 User Template 100
6.2.3 Server Template 101
6.2.4 Verifying Properties in UPPAAL 104
6.3 TLA+ Model 106
6.3.1 Properties and Results 113
6.4 Summary 114

7 NA-DOBAM Ontology 115
7.1 Preliminaries 116
7.2 Access Control Ontology for Rural BPO 118
7.2.1 NA-DOBAM Ontology 118
7.2.2 RBPO Scenarios 119

7.2.3 NA-DOBAM Ontologies for RBPO Scenarios 120
7.3 Access Control Information Retrieval and Rules 127
7.3.1 Retrieving Information from Ontologies 127
7.3.2 Separation of Duty and Delegation 130
7.3.3 Access Control Rules 131
7.4 Examples of NA-DOBAM Ontology for Federation 134
7.4.1 Multi-Institution Course Management System (MI-CMS) . . 134
7.4.2 Media Streaming Services (MSS) 136
7.5 Summary 138

8 Conclusions and Future Work **141**
8.1 Conclusions 141
8.2 Future Work 142

Appendix **143**

A Tools for Formal Modelling **143**
A.1 TLA+ 143
A.2 UPPAAL 145
A.3 Protégé 146
A.4 LINGO 147

B Formalisation of Good Enough Security **149**
B.1 Mathematical Formulation 150
B.1.1 Symbols Used in our Formulation 151
B.1.2 Model-1 152
B.1.3 Model-2 154
B.2 Scenarios 155
B.3 Results and Discussion 158
B.3.1 Model-1 Results 158
B.3.2 Model-2 Results 158
B.4 Summary 161

C Locating Distributed Objects in a Federation **163**
C.1 Discussion on Topology 164
C.2 Our Model 167
C.3 Analysis 168
C.3.1 Minimum Delay Path 169
C.3.2 Temporary Server Disconnection 171
C.4 Summary 173

Bibliography **175**

List of Figures

1.1 Models of Data Sharing over a Network 6

3.1 Organisation of a Rural BPO 32
3.2 Organisation of an MI-CMS 36
3.3 Organisation of a MSS 39
3.4 Video Streaming with Proxy 43

4.1 DOBAM Family 47
4.2 Core DOBAM 48
4.3 State Diagram of an Access Process 55
4.4 TLA+ Specification of the Policy in Example 4.3 60
4.5 Comparison of Number of Rules in DOBAM with TAC and RBAC 63
4.6 Comparison of Number of Rules in DOBAM with RBAC 63
4.7 Simulation Architecture 64
4.8 Authorisation time of DOBAM, RBAC and TAC 66
4.9 Comparison of Authorisation Time of DOBAM with RBAC 66

5.1 NA-RBAC model 70
5.2 Permission Update and Client Access with Network Disconnections 74
5.3 Block Diagram of the NA-RBAC Simulator 81
5.4 Confidence Interval of the request ratios for 10%, 50% and 80% network connection 83
5.5 Ratio of Requests Serviced by NA-RBAC to RBAC for Different Network Connection Percentages 84
5.6 Ratio of Correct to Total Client Permissions for Different Rate of Client Permission Updates 85
5.7 Comparison of HNA-RBAC to NA-RBAC and RBAC using Exponential Distribution for Different Network Connections 86
5.8 Useful Work Done in HNA-RBAC and RBAC for Different Network Connections 88
5.9 NA-DOBAM Family 89
5.10 Core NA-DOBAM 90

6.1 Network Template 100
6.2 User Template 100
6.3 Server Template 101
6.4 UPPAAL Simulator 105

6.5 User, Network and Server States . . . 107
6.6 Initial predicate . . . 107
6.7 Next-state action . . . 107
6.8 Send Action . . . 109
6.9 Accept Action . . . 109
6.10 Disconnect Network Action . . . 110
6.11 Reconnect Network Action . . . 110
6.12 Receive Data . . . 111
6.13 Reject Action . . . 111
6.14 Revoke Action . . . 111
6.15 Allow Permission Action . . . 112
6.16 Deny Permission Action . . . 112

7.1 Class Hierarchy of NA-DOBAM Ontology . . . 118
7.2 Object Properties of NA-DOBAM Ontology . . . 118
7.3 Scenario 1: Nationwide RBPO . . . 120
7.4 Scenario 2: Small regional RBPO . . . 120
7.5 Class Hierarchy of Client, client0 . . . 121
7.6 Object Properties of Client, client0 . . . 122
7.7 Class Hierarchy of RBPO Base Ontology, rbpo0 . . . 123
7.8 Restriction on User Class, rbpo0 . . . 123
7.9 Class Hierarchy of RBPO1 Ontology, rbpo1 . . . 124
7.10 Class Hierarchy of RBPO2 Ontology, rbpo2 . . . 125
7.11 Object Properties of RBPO1 Ontology, rbpo1 . . . 126
7.12 Restriction of QualityManager Class, rbpo1 . . . 126
7.13 Query Result for Example 1 . . . 128
7.14 Query Result for Example 2 . . . 129
7.15 Query Result for Example 3 . . . 130
7.16 Result of Rule 1 . . . 132
7.17 Class Hierarchy for MI-CMS . . . 135
7.18 Object Property for MI-CMS . . . 136
7.19 Data Property for MI-CMS . . . 136
7.20 Class Hierarchy for MSS . . . 137
7.21 Object Property for MSS . . . 138
7.22 Data Property for MSS . . . 138

B.1 LINGO Model for Model-1 . . . 154

C.1 Service Topology . . . 165
C.2 Working of the Model . . . 167
C.3 Interaction Diagram of the Model . . . 169
C.4 Minimum Delay Path . . . 170
C.5 State Diagram for the Local Server Status . . . 170
C.6 Availability vs Disconnection Probability of Local Servers . . . 172
C.7 Expected Time for Object Look-up . . . 173

List of Tables

2.1 Comparison of ACMs for Scenarios involving Object Decomposition 20
2.2 Comparison of ACMs for Network Awareness and Distributed Access Control 23
2.3 Comparison of Ontologies for Federation Support 26

4.1 Notations in DOBAM 48
4.2 TLA+ Specification 58
4.3 Parameters for Comparing the Number of Rules 62

5.1 Notations in NA-RBAC 71
5.2 TLA+ Specification 76
5.3 Notations in the Analytical Model 80
5.4 Simulation Parameters 82
5.5 TLA+ Specification 93

A.1 Operators in TLA+ 145
A.2 Properties with Examples 147
A.3 LINGO Syntax for Some Maths Notations 148

B.1 Result of Model-1 159
B.2 Result of Model-2 160