

**AUTHORIZATION FOR WORKLOADS IN A  
DYNAMICALLY SCALING, HETEROGENEOUS  
SYSTEM**

Pushpalanka Rajaluxmie Jayawardhana

158217G

Degree of Master of Science

Department of Computer Science and Engineering

University of Moratuwa

Sri Lanka

April 2019

**AUTHORIZATION FOR WORKLOADS IN A  
DYNAMICALLY SCALING, HETEROGENEOUS  
SYSTEM**

Pushpalanka Rajaluxmie Jayawardhana

158217G

Thesis submitted in partial fulfillment of the requirements for the degree Master  
of Science

Department of Computer Science and Engineering

University of Moratuwa

Sri Lanka

April 2019

## DECLARATION

I declare that this is my own work and this thesis does not incorporate without acknowledgment any material previously submitted for a Degree or Diploma in any other University or institute of higher learning and to the best of my knowledge and belief, it does not contain any material previously published or written by another person except where the acknowledgment is made in the text.

In addition, I hereby grant to the University of Moratuwa the non-exclusive right to reproduce and distribute my thesis, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works.

.....  
Pushpalanka Rajaluxmie Jayawardhana

.....  
Date

The above candidate has carried out research for the Masters thesis under my supervision.

.....  
Prof. Gihan Dias

.....  
Date

## **ABSTRACT**

Enterprises in the modern world have gone through a phase of digital transformation which has contributed immensely in the growth of enterprise systems. This has spread through concepts such as e-government, open banking, e-healthcare, e-commerce concepts to digitalized organizations. Conventionally, systems ran within the corporate infrastructure. In the past few years, organizations have been moving to the cloud. Authentication and authorization work well in on-premises or within a single cloud. But authentication and authorization in modern systems with hybrid cloud and multi-cloud approaches where none of the parties individually govern the perimeter of the system is still an open problem. The components serving in one part of the system can be totally strange to the other party and is not aware of the security privileges they have. On the other hand, enterprise systems cannot compromise on information security, though they may want to have the advantages of multi-cloud systems. While there have been several attempts done by the research communities from Google, Docker, Dropbox etc. to provide a common identification protocol across systems, authorization mechanisms still lacks attention. This research provides a solution for authorization between multiple systems (on-premise and cloud or multiple clouds) based on identification completed by the infrastructure. In the provided solution, a central server assigns attested identity to each legitimate workload, to identify them and apply authorization policies at resource access. The resource servers reside behind an access control layer, which allows method execution according to an administrator-defined policy that considers fine-grained details such as the accessing resource, action to be performed and other context details, in addition to the identity of the consumer and the resource.

**Keywords:** Authorization, Access control, Multi-Cloud, Hybrid Cloud

## **ACKNOWLEDGMENTS**

I would like to express profound gratitude to my supervisor, Prof. Gihan Dias, for his continued supervision, invaluable support, useful suggestions throughout the research work and forewarnings on possible pitfalls. His experience, expertise, and continuous guidance encouraged and enabled me to complete this research work successfully.

I also express my gratitude to Mr. Prabath Siriwardena, my external project supervisor for providing me with the initial project idea, giving invaluable assistance throughout and introducing me to the direct technical community around latest technologies relevant to the project. It was a great identification of an emerging industrial requirement, which I could passionately work on to provide a solution.

I am grateful for all the support given by Dr. Indika Perera, to complete this research project, with smooth handling of all the processes. I am extending my thanks to all the staff from the Department of Computer Science and Engineering for their kindness expressed in all occasions.

I would like to thank WSO2 Lanka (PVT) Ltd, for the encouragement given on proceeding with higher education and sponsorship given to follow the MSc. I am thankful to my colleagues and friends for their continued assistance and encouragement. I would like to especially thank Mr. Chamila Wijayarathna for helping me to get research materials.

I am as ever, especially indebted to my parents for their support throughout my life. Their love and blessings kept me encouraged at the hardest times to complete this project, despite the obstacles.

# TABLE OF CONTENTS

|  |             |
|--|-------------|
| <b>DECLARATION</b>   | <b>i</b>    |
| <b>ABSTRACT</b>  | <b>ii</b>   |
| <b>ACKNOWLEDGMENTS</b>   | <b>iii</b>  |
| <b>TABLE OF CONTENTS</b>   | <b>iv</b>   |
| <b>LIST OF FIGURES</b>   | <b>vii</b>  |
| <b>LIST OF TABLES</b>  | <b>viii</b> |
| <b>LIST OF ABBREVIATIONS</b>   | <b>ix</b>   |
| <b>1. INTRODUCTION</b>   | <b>1</b>    |
| 1.1 Multi-cloud Environments   | 2           |
| 1.2 Problem Statement  | 3           |
| 1.3 Objectives   | 6           |
| 1.4 Research Contribution  | 6           |
| 1.5 Outline  | 7           |
| <b>2. LITERATURE REVIEW</b>  | <b>9</b>    |
| 2.1 Access Control   | 9           |
| 2.2 Authentication   | 10          |
| 2.3 Authorization  | 11          |
| 2.3.1 Access Control Matrix  | 11          |
| 2.3.1.1 Access Control List  | 12          |
| 2.3.2 Discretionary Access Control (DAC)                                 | 13          |
| 2.3.3 Mandatory Access Control (MAC)                                     | 13          |
| 2.3.4 Role Based Access Control (RBAC)                                   | 13          |
| 2.3.5 Attribute-Based Access Control (ABAC)                              | 14          |
| 2.3.5.1 XACML  | 14          |
| 2.3.5.2 OPA  | 17          |
| 2.4 Lattice Based Access Control - Classical Information Security Models | 18          |
| 2.4.1 Bell-La-Padula Model   | 20          |
| 2.4.2 BIBA Model   | 21          |
| 2.4.3 Chinese Wall Model   | 23          |
| 2.4.4 Clark-Wilson Model   | 24          |
| 2.4.5 Graham-Denning Model   | 26          |

|           |   |           |
|-----------|---|-----------|
| 2.4.6     | Harrison-Ruzzo-Ullman Model                               | 27        |
| 2.4.7     | Take-Grant Model  | 28        |
| 2.5       | Cloud Computing   | 29        |
| 2.5.1     | History   | 29        |
| 2.5.2     | Cloud Services  | 29        |
| 2.5.3     | Hyper-Converged Cloud                                     | 30        |
| 2.6       | Workloads   | 31        |
| 2.6.1     | What is a workload?                                       | 31        |
| 2.7       | Workload Authentication Technologies                      | 31        |
| 2.7.1     | Challenge Response Authentication Mechanisms              | 32        |
| 2.7.1.1   | Username and password based authentication                | 32        |
| 2.7.2     | Needham–Schroeder protocol                                | 32        |
| 2.7.3     | Kerberos protocol   | 34        |
| 2.7.4     | The platform provided privileged API based authentication | 37        |
| 2.7.4.1   | Amazon EC2 IID  | 37        |
| 2.7.4.2   | Google Cloud Provider IIT                                 | 38        |
| 2.7.4.3   | Microsoft Azure MSI                                       | 39        |
| 2.7.5     | SPIFFE standard   | 40        |
| 2.7.5.1   | SPIFFE in action  | 41        |
| 2.7.5.2   | SPIFFE implementations                                    | 44        |
| 2.8       | Workload Authorization Technologies                       | 45        |
| 2.8.1     | OAuth 2.0 Authorization Framework                         | 46        |
| 2.8.1.1   | OAuth 1.0 vs OAuth 2.0                                    | 46        |
| 2.8.1.2   | OAuth 2.0   | 47        |
| 2.8.1.3   | Fine-grained authorization with OAuth2 scopes             | 49        |
| 2.8.1.4   | OAuth 2.0 popularity                                      | 50        |
| 2.8.2     | Authorization Servers                                     | 51        |
| <b>3.</b> | <b>SOLUTION DESIGN</b>                                    | <b>52</b> |
| 3.1       | Methodology   | 54        |
| 3.1.1     | Authentication technology                                 | 54        |
| 3.1.2     | Authorization Technologies                                | 56        |
| 3.1.2.1   | DAC vs MAC  | 56        |
| 3.1.2.2   | RBAC vs ABAC  | 57        |
| 3.1.2.3   | XACML vs OPA  | 57        |
| 3.1.2.4   | Authentication and Authorization                          | 59        |
| 3.1.3     | Authorization Server                                      | 62        |
| 3.2       | Architecture  | 62        |

|   |           |
|---|-----------|
| 3.2.1 Interactions                                  | 64        |
| 3.2.2 Assumptions                                   | 64        |
| <b>4. SOLUTION IMPLEMENTATION</b>                   | <b>66</b> |
| 4.1 Pre Resource Access - OAuth2 Token Issuing Flow | 68        |
| 4.2 Resource Access - OAuth2 Token Validation Flow  | 74        |
| <b>5. SOLUTION EVALUATION</b>                       | <b>77</b> |
| 5.1 Deployment Model                                | 77        |
| 5.2 Deployment Configuration                        | 79        |
| 5.2.1 Infrastructure                                | 79        |
| 5.2.2 Policies                                      | 79        |
| 5.2.3 Test cases                                    | 83        |
| 5.2.3.1 Correctness                                 | 83        |
| 5.2.3.2 Performance                                 | 84        |
| <b>6. CONCLUSION AND FUTURE WORK</b>                | <b>86</b> |
| 6.1 Conclusion                                      | 86        |
| 6.2 Limitations                                     | 87        |
| 6.3 Future Work                                     | 88        |
| <b>REFERENCES</b>                                   | <b>90</b> |
| <b>APPENDIX</b>                                     | <b>95</b> |
| Sample XACML Policy                                 | 95        |
| Sample OPA policy                                   | 97        |
| Sample SPIFFE SVID X.509 certificate                | 98        |



## **LIST OF FIGURES**

|   |    |
|---|----|
| Figure 1.1 - Cloud Usage Plans                                      | 3  |
| Figure 1.2 - A Multi-cloud Environment Used by an Enterprise System | 3  |
| Figure 2.1 - Access Control and Other Security Services             | 9  |
| Figure 2.2 - Access Matrix  | 11 |
| Figure 2.3 - Access Control List for Files                          | 12 |
| Figure 2.4 - XACML Based Access Control Components                  | 15 |
| Figure 2.5 - How OPA works  | 17 |
| Figure 2.6 - Access Control Matrix of Graham-Denning Model          | 27 |
| Figure 2.7 - History of Cloud Computing                             | 29 |
| Figure 2.8 - Hyper-Converged Cloud                                  | 30 |
| Figure 2.9 - Kerberos Protocol                                      | 35 |
| Figure 2.10 - Platform Mediated Authentication                      | 37 |
| Figure 2.11 - Azure Instance Authentication                         | 40 |
| Figure 2.12 - SPIFFE in action                                      | 47 |
| Figure 2.13 - Client Credentials Grant                              | 48 |
| Figure 3.1 - Approach 1 for SPIFFE and OPA Integration              | 59 |
| Figure 3.2 - Common Model   | 60 |
| Figure 3.3 - Approach 2 with Authorization Server                   | 61 |
| Figure 3.4 - Architectural Design                                   | 63 |
| Figure 4.1 - Implementation Scope                                   | 66 |
| Figure 4.2 - Workload Gets an OAuth2 Token                          | 68 |
| Figure 4.3 - SPIFFE Based OAuth Client Authenticator                | 70 |
| Figure 4.4 - OPA Based OAuth2 Scope Handler Implementation          | 71 |
| Figure 4.5 - Workload Access Another Workload                       | 74 |
| Figure 4.6 - OPA Based OAuth2 Token Validator                       | 75 |
| Figure 5.1 - Deployment for Evaluation                              | 77 |

## **LIST OF TABLES**

|   |    |
|---|----|
| Table 2.1 - Attestation Policy for SPIFFE IDs             | 42 |
| Table 2.2 - Access Control Technologies Comparison        | 45 |
| Table 3.1 - Workload Authentication Technology Comparison | 55 |
| Table 3.2 - ABAC Technology Comparison                    | 58 |
| Table 5.1 - Test Cases                                    | 83 |

## **LIST OF ABBREVIATIONS**

|        |   |
|--------|---|
| ABAC   | - Attribute Based Access Control                    |
| CI/CD  | - Continuous Integration/Continuous Development     |
| CRAM   | - Challenge Response Authentication Mechanisms      |
| CNCF   | - Cloud Native Computing Foundation                 |
| DAC    | - Discretionary Access Control                      |
| DCR    | - Dynamic Client Registration                       |
| GDPR   | - General Data Protection Regulation                |
| IAM    | - Identity and Access Management                    |
| IID    | - Instance Identity Document                        |
| IIT    | - Instance Identity Token                           |
| MAC    | - Mandatory Access Control                          |
| MSA    | - Micro-Services Architecture                       |
| MSI    | - Managed Service Identity                          |
| OPA    | - Open Policy Agent                                 |
| PAP    | - Policy Administration Point                       |
| PDP    | - Policy Decision Point                             |
| PEP    | - Policy Enforcement Point                          |
| PIP    | - Policy Information Point                          |
| RBAC   | - Role Based Access Control                         |
| SaaS   | - Software as a Service                             |
| SPIFFE | - Secure Production Identity Framework For Everyone |
| SPIRE  | - SPIFFE Runtime Environment                        |
| STS    | - Security Token Service                            |
| SVID   | - SPIFFE Identity and Verifiable Identity Document  |
| XACML  | - eXtensible Access Control Markup Language         |