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

LIST OF FIGURES

LIST OF TABLES

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