REINFORCEMENT LEARNING-BASED SECURITY VULNERABILITY DETECTION FOR MICROSERVICES

Kasun Maduranga

(219361N)

Degree of Master of Science

Department of Computer Science and Engineering

University of Moratuwa

Sri Lanka

July 2025

REINFORCEMENT LEARNING-BASED SECURITY VULNERABILITY DETECTION FOR MICROSERVICES

Kasun Maduranga

(219361N)

MSc thesis submitted in partial fulfilment of the requirement for the degree Master of Science.

Department of Computer Science and Engineering

University of Moratuwa

Sri Lanka

July 2025

DECLARATION

I declare that this is my own work, and this MSc Research Project Report does not incorporate without acknowledgement 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 acknowledgement is made in the text.

Also, I hereby grant to the University of Moratuwa the non-exclusive right to reproduce and distribute my thesis/dissertation, 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.

……. 02/07/2025

Kasun Maduranga Date

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

Name of the supervisor: Prof. Indika Perera

……. 02/07/2025

Prof. Indika Perera Date

ACKNOWLEDGEMENT

I like to express my sincere gratitude to my thesis supervisor, Professor Indika Perera, for his unwavering support and essential direction during my study. His expertise in the field and encouragement provided was vital to the successful finalization of this work. I would like to mention the remarkable flexibility that Professor Indika Perera and the Computer Science and Engineering department provided for the completion of this research.

I extend my heartfelt thanks to the Google Cloud Platform developers for creating the Online Boutique microservice application. I appreciate the contributions they have made to the industry and academic community by releasing this application as an open-source project and maintaining it actively. It made the implementation of the proposed methodology feasible and convenient.

Lastly, I like to convey my appreciation towards my parents and my wife for their patience and continuous support. They always kept me motivated to complete this research successfully.

ABSTRACT

Microservices architecture (MSA) is the main architectural model for contemporary software systems due to its scalability, flexibility, and maintainability. Yet, there are major security concerns that emerge from the distributed and dynamic nature of microservices. Most of these risks and vulnerabilities are difficult to identify due to the complexity and the evolving nature of microservice based systems. Due to this reason, conventional security vulnerability detection methods designed for monolithic systems are inadequate and ineffective in microservice based systems. To address this shortcoming, this thesis investigates the use of Reinforcement Learning (RL) and offers a Proximal Policy Optimization (PPO)-based framework as an automated and adaptive tool for finding security vulnerabilities in microservices. “Online Boutique” application, which built on microservices architecture is utilized as a testbed for assessing the performance of the developed RL framework in finding security vulnerabilities. The PPO agent learns to interact with the system, simulate attacks, and find real-time security vulnerabilities. The study intends to mimic DoS attack situations targeting the Online Boutique application. The suggested approach is a scalable, consistent security testing tool able to evolve to identify developing threats and adapt to new security vulnerabilities. This study proposes a promising substitute for conventional manual testing for DoS attacks. The results illustrate the efficacy of the PPO framework in detecting vulnerabilities in the microservices environment, with implications for improving the security of microservices-based applications.

Keywords: Microservices Architecture, Reinforcement Learning, Proximal Policy Optimization, Vulnerability Detection, Security Testing, Automated Security, Penetration Testing, DoS Simulation, Machine Learning in Cybersecurity.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

MSA	Microservice Architecture
RL	Reinforcement Learning
PPO	Proximal Policy Optimization
DoS	Denial of Service
SQL	Structured Query Language
URL	Uniform Resource Locator
CPU	Central Processing Unit
API	Application Programming Interface
TLS	Transport Layer Security
DQN	Deep Q-Networks
IDS	Intrusion Detection Systems
TRPO	Trust Region Policy Optimization
CI	Continuous Integration
CD	Continuous Deployment
XSS	Cross-Site Scripting
A3C	Asynchronous Advantage Actor-Critic
RAM	Random Access Memory
GB	Giga Byte
MB	Mega Byte
KB	Kilo Byte
BIOS	Basic Input/Output System
UEFI	Unified Extensible Firmware Interface
LTS	Long Term Support
WSL	Windows Subsystem for Linux
CLI	Command Line Interface

IP	Internet Protocol
HTTP	Hyper Text Transfer Protocol
ID	Identifier
JSON	JavaScript Object Notation
QPS	Queries Per Second
TCP	Transmission Control Protocol
GAE	Generalized Advantage Estimator
UI	User Interface