INFORMATICS INSTITUTE OF TECHNOLOGY

In Collaboration with

UNIVERSITY OF WESTMINSTER (UOW)

ARGUS -
An independent and intelligent Intrusion Detection and Prevention Solution for AWS based Applications.

A dissertation By

N.G.J. Jayasanka

Supervised By

Mr. Chathushka Dilhan

Submitted in partial fulfillment of the requirements for the BSc (Hons) Software Engineering degree.

Department of Computing

May 2018

Abstract

Cloud Computing has become very popular throughout the years because of its ease of use, Specially when it comes to Big Data solutions. It has become a multi-billion-dollar industry but it has become a major target of the attackers because of the huge amount of data that the attackers can get their hands on to. This project mainly addresses security aspects in the cloud. The prototype will be focused on Amazon Web Services (AWS) based applications. The prototype would be built according to 'Shared Responsibility Model' of AWS. The proposed solution focuses on how to apply application log monitoring for Amazon Web Services (AWS) Infrastructure as a Service (IaaS) environments. The proposed solution consists of few Machine Learning Components in order to detect and prevent intrusions. The prototype will use AWS CloudTrail and AWS ClourWatch Logs which are stored and mined for suspicious events.