**MSc Final Project Outline**

**Research area**

Cloud infrastructure security policies.

**Working title**

An ontological framework for dynamic security policy application in public cloud.

**Proposed Research Problem**

The increased use of public cloud for business workloads has led to the need for dynamic infrastructure security policies that are tailored to the needs of a business. Custom policies can be utilised to reflect internal policy whilst industry benchmarks, such as Center for Internet Security (CIS), can reflect cutting edge security best practice on various cloud platforms. Furthermore, regulatory benchmarks, such as Payment Card Industry Data Security Standard (PCI DSS), can also be employed. A dynamic framework for merging these different security policy sets is required to avoid duplication of alerting, ensure full coverage and more easily keep pace with changes in industry best practice.

**Research Question(s)**

1. Can ontologies be used as a basis for a dynamic cloud security policy framework?
2. How can ontological security policies be prioritised to reflect specified business requirements?

**Proposed Aims**

The aim of this project is to determine how ontologies could be used to create a dynamic mechanism for applying optimal security policies based on a business use case.

**Proposed Objectives**

1. Create or utilise an existing ontology to define cloud security policies based on a financial services use case.
2. Develop a hierarchical mechanism to determine security policies to be applied based on the use case.

**Proposed Research Design**

1. Review previous literature on and around this subject.
2. Identify suitable ontological approaches.
3. Develop an ontology to suit this use case.
4. Evaluate the ontology using a sample of custom and CIS security policies on Microsoft Azure.
5. Document and share findings.

**Artefact(s) that can be created**

* An ontology (if no suitable ontology identified in literature).
* A dynamic framework for prioritising and deduplicating the policies based on the chosen ontology.