University of Victoria | Graduate Studies

Notice of the Final Oral Examination for the Degree of Doctor of Philosophy

of

FAHAD F. ALRUWAILI

MSc (Claremont Graduate University, 2011)
MSc (DePaul University, 2008)
BSc (King Fahd University of Petroleum and Minerals, 2002)

"Information Security, Privacy, and Compliance Models for Cloud Computing Services"

Department of Electrical and Computer Engineering

Thursday, April 7, 2016
9:30 A.M.
Engineering and Computer Science Building
Room 468

Supervisory Committee:
Dr. T. Aaron Gulliver, Department of Electrical and Computer Engineering, University of Victoria (Supervisor)
Dr. Daler N. Rakhmatov, Department of Electrical and Computer Engineering, UVic (Member)
Dr. Sudhakar Ganti, Department of Computer Science, UVic (Outside Member)

External Examiner:
Dr. Hilal Hussain, Senior Systems Development Specialist, IRTI

Chair of Oral Examination:
Dr. McGinnis-Archibald, Department of Linguistics, UVic

Dr. David Capson, Dean, Faculty of Graduate Studies

Abstract

The recent emergence and rapid advancement of Cloud Computing (CC) infrastructure and services made outsourcing Information Technology (IT) and digital services to Cloud Providers (CPs) attractive. Cloud offerings enable reduction in IT resources (hardware, software, services, support, and staffing), and provide flexibility and agility in resource allocation, data and resource delivery, fault-tolerance, and scalability. However, the current standards and guidelines adopted by many CPs are tailored to address functionality (such as availability, speed, and utilization) and design requirements (such as integration), rather than protection against cyber-attacks and associated security issues. In order to achieve sustainable trust for cloud services with minimal risks and impacts on cloud customers, more appropriate cloud information security models are required. The research described in the dissertation details the processes adopted for the development and implementation of an integrated information security cloud based approach to cloud service models. This involved detailed investigation into resolution of some of the inherent information security deficiencies identified in the existing cloud service models, service agreements, and compliance issues. The research conducted was a multidisciplinary in nature, with detailed investigations on factors such as people, technology, security, privacy, and compliance involved in cloud risk assessment to ensure all aspects are addressed in a holistic and well-structured models.

The primary research objectives for this thesis were investigated through a series of scientific papers centered on these key research disciplines. The assessment of information security, privacy, and compliance implementations in cloud environment was achieved throughout the studies undertaken and described in Chapters two, three, four, and five. Paper 1 *(CCIPS: A Cooperative Intrusion Detection and Prevention Framework for Cloud Services)* outlines a framework for detecting and preventing known and zero-day threats targeting cloud computing networks. This framework formed the basis for implementing enhanced threat detection and prevention via behavioral and anomaly data analysis. Paper 2 *(A Trusted CCIPS Framework)* extends the work of cooperative intrusion detection and prevention to enable trusted delivery of cloud services. The trusted CCIPS model details and justifies the multi-layer approach to enhance the performance and efficiency of detecting and preventing cloud threats. Paper 3 *(SOCaaS: Security Operations Center as a Service for Cloud Computing Environments*) describes the need for a trusted third party to perform real-time monitoring of cloud services to ensure compliance with security requirements by suggesting a security operations center system architecture. Paper 4 *(SecSLA: A Proactive and Secure Service Level Agreement Framework for*

Cloud Services) identifies the necessary cloud security and privacy controls that need to need to be addressed in the contractual agreement i.e., service level agreement (SLA), between CPs and their customers.

Paper five, six, seven, and eight (Chapters 6 – 9) focus on addressing and reducing the risk issues resulting from poor assessment to the adoption of cloud services and the different factors that influence such strategic migration. The investigation of cloud-specific information security risk management and migration readiness frameworks, detailed in Paper 5 *(An Effective Risk Management Framework for Cloud Computing Services)* and Paper 6 *(Information Security, Privacy, and Compliance Readiness Model)* was achieved through extensive consideration of all possible factors from different studies. Analysis of the resulting investigation indicated that several key factors, including risk tolerance, can significantly influence the migration decision to cloud technology. An additional issue found during this research in assessing the organization's readiness to move to the cloud was the necessity to ensure that the respective cloud service provider was actually compliant with information security, privacy, and compliance (ISPC) requirements. The investigation is extended in Paper 7 *(A Practical Life Cycle Approach for Cloud based Information Security)* to include the six phases of creating proactive cloud information security system beginning with initial design, through the development, and implementation phase to the operations and maintenance. The inherent difficulty in identifying ISPC compliant cloud technology was resolved by employing a source of tracking method, namely eligibility and verification system Paper 8 *(Cloud Services Information Security and Privacy Eligibility and Verification System).*

Finally, Paper 9 *(A Case Study of Migration to a Compliant Cloud Technology)* describes the actual implementation of combining the proposed frameworks and models, as discussed through the previous 7 papers, to help the decision making process faced by the Saudi financial agency migrate their IT services to the cloud. Together these models and frameworks suggest that the threats and risks associated with cloud services are continuously changing and importantly, increasing in complexity and sophistication, contribute to make stronger cloud based information security, privacy, and compliance technological frameworks. The outcomes published in this research have significantly contributed to knowledge of best practices in ensuring information security controls are addressed, monitoring, enforced, and compliant with relevant regulations.