Chapter 6
IT Security and Governance Compliant Service Oriented Computing in Cloud Computing Environments

Hussain Al-Aqrabi
University of Derby, UK

Lu Liu
University of Derby, UK

ABSTRACT
The authors present the key security challenges and solutions on the Cloud with the help of literature reviews and an experimental model created on OPNET that is simulated to produce useful statistics to establish the approach that the Cloud computing service providers should take to provide optimal security and compliance. The literature recommends the concept of unified threat management for ensuring secured services on the Cloud. Through the simulation results, the authors demonstrate that UTM may not be a feasible approach to security implementation as it may become a bottleneck for the application Clouds. The fundamental benefits of Cloud computing (resources on demand and high elasticity) may be diluted if UTMs do not scale up effectively as per the traffic loads on the application Clouds. Moreover, it is not feasible for application Clouds to absorb the performance degradation for security and compliance because UTM will not be a total solution for security and compliance. Applications also share the vulnerabilities just like the systems, which will be out of UTM Cloud’s control.

INTRODUCTION
The evolution of the concept of Cloud computing has changed the way businesses look at IT for fulfilling their needs. IT is now viewed as a massive implementation of integrated hardware, software, platforms and networking from where the businesses can purchase services as per what they need. A Cloud can be viewed as a hypermarket of IT services available at affordable prices based on needs and demands. Hence, it appears that Cloud computing concept has emerged at the right time...
when such companies were formulating multi-
million dollar budgets to upgrade their hardware
and software systems. But is Cloud computing
ready to the extent that it can be considered as an
alternative to hardware and software upgrades, or
as an alternative to deployment of new IT systems?
Many scholars argue that Cloud is ready, but the
most significant challenge is related to security
and compliance.

With the growing popularity of Cloud comput-
ing, the concerns about security and compliance
are also growing. Al-Aqrabi et al. (2012) describes
that Cloud computing is gradually gaining popu-
larity among businesses of all types and sizes due
to the numerous advantages over self-hosted IT
infrastructures (p.1). Businesses do not want to
be deprived of the already established and ac-
cepted benefits of Cloud computing and hence
they require continuous research towards the path
to achieve standardised policies and controls on
Cloud computing that shall be acceptable to the
regulatory bodies (Carroll, Merve and Kotze,
2011, p. 1). It is important for the management
of a business to understand what threats and risks
exist on Cloud computing infrastructures and
what are the feasible mitigation strategies (Car-
roll, Merve and Kotze, 2011, p. 2). In a survey
conducted by Carroll, Merve and Kotze (2011, p.
4), it was observed that the IT managers stated
information security, business continuity and
regulatory compliance as the top three concerns
in moving their business workflows to the Cloud.
Ramgovind, Eloff and Smith (2010, p. 1) argued
that the full potential of Cloud computing cannot
be used for the benefit of businesses unless the
security and compliance issues are sorted out.
They further elaborated that secured connectivity
to Clouds over Internet, data segregation, data
location and multi-tenancy are the key issues that
are discussed by Gartner and IDC reports on Cloud
computing security that are coming in the way of
achieving full compliance to the established regu-
lations and acts (p. 3). The main security issues
to be solved in the context of connectivity, data
segregation, data location and multi-tenancy are:

- identity management, authentication, authorisa-
tion, confidentiality, integrity, non-repudiation
and availability (Ramgovind, Eloff and Smith,
2010, p. 3).

- At the technical level, Mukhin and
Volokyata (2011, p. 738-739) described that Cloud
computing comprises new types of vulnerabilities,
like – incorrect provisioning in virtualisation,
riding and hijacking of virtual sessions, insecure
or obsolete cryptography keys, evasion of billing/
metering data, data recovery of one user when the
resource gets allocated to another user, insufficient
virtual network controls, poor authentication and
authorisation in the virtual machines, etc. The
author has presented this study with the help of
background and contextual reviews of Cloud com-
puting security, and a modelling and simulation
based experiment to test the feasibility of using
security-as-a-service by a separate Cloud provider
using unified threat management solutions. The
findings of the experiment have been compared
with the literature review outcomes to present the
conclusions and recommendations. The chapter
has been divided into seven sections: the first four
sections dedicated to literature review and critical
discussions, the next two sections to present the
model and analysing its results and the last section
to present the conclusions.

**BACKGROUND**

**Cloud Computing Domains**

The architecture, deployment, workflows and
service procedures of Cloud computing is yet
to be standardised. The academic scholars and
professional architects have presented their own
architectures of Cloud computing in numerous
research papers. (Qian, Luo, Du and Guo, 2009,
p. 626). NIST has come forward with a draft paper
to standardise Cloud computing, albeit currently
at high level only. In the NIST’s model, Cloud has
been presented as an integrated service oriented
architecture comprising three forms of offerings
– software-as-a-service (SaaS), platform-as-a-
Related Content

Marketing of Tourism Industry: Enhancing Services through Marketing Mix Elements
www.igi-global.com/chapter/marketing-of-tourism-industry/179995?camid=4v1a

Constraint Satisfaction for Planning and Scheduling
www.igi-global.com/chapter/constraint-satisfaction-planning-scheduling/24467?camid=4v1a

Securing Data Storage By Extending Role-Based Access Control
www.igi-global.com/article/securing-data-storage-by-extending-role-based-access-control/105508?camid=4v1a

Coordination in Multi-Agent Planning with an Application in Logistics
www.igi-global.com/chapter/coordination-multi-agent-planning-application/24463?camid=4v1a