Chapter 55
Cloud Crime and Fraud:
A Study of Challenges for Cloud Security and Forensics

Nimisha Singh
Birla Institute of Management Technology, India

ABSTRACT

Changing trends in IT industry are opening new avenues. With the scalability, flexibility, and economic advantage offered by cloud computing, more and more organizations are moving towards cloud for their applications. With all the benefits of cloud computing, it poses a danger of digital crime and security breaches. These challenges are compounded by the fact that cybercrime and the transgressors transcend geographical boundaries while the law enforcement does not. This paper tries to focus on how cloud computing is rising to the challenges thrown in from cyber space and recent developments to avoid and mitigate cloud fraud and abuse. Taking counter measures at organizational level, will alleviate and up to an extent eliminate security breaches. With current knowledge on policy and standards adopted by developed nations, the policy makers and law enforcement agencies in developing countries can work towards formulating standards and guidelines for awareness on threats, vulnerabilities and effectiveness of security controls to respond to risk.

INTRODUCTION

Cloud based IT services have been gaining popularity as they do not require big investments. Ford (2011) described the cloud as "in which dynamically scalable and often-virtualized resources are provided as a service over the internet" whereas Knorr & Gruman (2009) described it as "any IT resources outside of the firewall including conventional outsourcing". Cloud services are based on a new business model of on demand service where customers can choose what they want, how much they want and pay only for those services, which they require and has been rendered to them. The shared use of resources like - storage, servers, and applications and services- has led to potential cost saving.

Even though the cloud technology is not mature, there is an increased confidence in its adoption by businesses owing to lower running costs and ease in deployment. Cloud computing offers flexibility,

DOI: 10.4018/978-1-5225-8897-9.ch055

efficiency and cost saving and at the same time poses challenges of security not only to users but also to regulatory and law enforcement agencies. The cloud service provider is entrusted with hosting, maintaining and has general access to customer data. Outsourcing and global dispersion of cloud service providers raises jurisdiction issue for law enforcement agencies since the service provider may have data centres in multiple countries, each with their unique laws on data usage and privacy. The layered architecture and multi-tenancy opens a large surface for attack from outsiders. With increasing trend towards adoption of cloud based services, there is a need for secure cloud services. Also, organizations are required to follow data governance law of their country which emphasize maintaining data privacy and confidentiality. The security in cloud environment needs to be evaluated from different perspectives:

- Cross border jurisdiction as the service provider may be in a different jurisdiction than the customer.
- Technical solution to make architecture more robust and difficult to penetrate by intruders.
- Compliance by organizations to maintain data privacy and confidentiality.

The paper looks at current state of affairs, cloud demand and risks; and offers advice on cloud adoption by incorporating technical, organizational and legal dimension to combat security issues. With technology available to today and process improvement, organizations can make themselves better prepared to tackle privacy and security breaches.

The chapter focuses on security and privacy issues raised by the cloud environment, investigation challenges in the cloud environment, different dimensions to cloud security so that organizations can be better prepared for secure information management in the cloud environment.

BACKGROUND

With Information technology playing a strong role in today's global economy, organizations are adopting cloud based services to develop and protect their market share in their core business. The survey of cloud service market indicates inexorable shift to cloud with IDC predicting public IT cloud service spending to grow to $127 billion by 2018 (Leopold 2014). IDC also predicts that "public IT cloud services will account for more than half of global software, server, and storage spending growth by 2018" (Leopold 2014). Driving this growth will be use of cloud based applications. Using cloud service, data will be outsourced to a cloud service provider which requires higher security standards to protect customer's data from losses due to technical malfunction, external intrusion and maintain confidentiality. As dispersion of cloud service providers enables low cost, flexibility and data availability, it also brings in jurisdiction issues in case of a security breach.

To understand how cloud environment has brought cost saving and flexibility, it is necessary to understand its characteristics, deployment model and service models. the As given by NIST, cloud computing is defined as a collection of five essential characteristics, three service models and four deployment models (Mell, 2011).

The essential characteristics are:

1. **On Demand Self-Service:** Provisioning of computing capabilities such as network storage, server time by consumer without human intervention by the service provider.