

## **Dr. Mohan Dhawan**

IBM Research Labs, India

Abstract of talk

### **“Security in a virtualized world”**

Cloud computing is a rapidly evolving landscape; and one that requires us to stay current or fall behind. The development of the cloud service model delivers business-supporting technology more efficiently than ever before. The shift from server to service-based thinking has transformed the way we think about designing, and delivering computing technology and applications. Although shifting to cloud technologies exclusively is affordable and fast, doing so undermines important enterprise-level security policies, processes, and best practices. These advances have created new security challenges and vulnerabilities, including security issues whose full impact is still emerging. In the absence of these standards, enterprises are vulnerable to security breaches that can quickly erase any gains made by embracing the cloud computing paradigm.

Understanding the impact of the differences between service models and how they are deployed is critical to managing the risk posture of an organization. A central component of managing risks in cloud computing is to understand the nature of security threats. While there are many vulnerabilities to cloud security, today we will focus exclusively on threats related to the shared, and on-demand nature of cloud computing. Among the most significant security risks associated with shared technology issues in cloud computing are data breaches, use of insecure APIs, possible malicious insiders in organizations, etc.

The security and privacy landscape is rapidly changing for both cloud providers and consumers. In today's settings, the consumers only have coarse grained security controls that relate to the operating system, applications, and data. This stems mostly from the abstraction of infrastructure, and the lack of visibility and capability to integrate many familiar fine-grained security controls. In this talk, I will enumerate several security risks associated with enterprise-level cloud computing and also discuss a novel cloud computing model that addresses several of the shortcomings of the shared infrastructure in the current cloud settings, and also allows providers and clients to establish mutually trusted services.

---