Data Security for Software as a Service

Pradeep Kumar Tiwari, Department of Computer Science and Engineering, Manipal University, Jaipur, India

Sandeep Joshi, Department of Computer Science and Engineering, Manipal University, Jaipur, India

ABSTRACT

Cloud computing is a BUZZ word of modern computing scenario. Cloud computing services are flexible and cost effective with resource utilization. Cloud computing have three service models SaaS (Software as a Service) PaaS (Plateform as a Service) and Iaas (Infrastructure as a Service). SaaS provide on demand application services such as email, ERP and CRM etc. Multi user can access applications and they can interact to each other at same time. All users data can be reside at same place. This flexibility of SaaS service also gives the security breaches. Loop holes of SaaS harder to find and maintain. The authors discuss here security vulnerabilities of SaaS with possible solutions. This study would be helpful to elaborate to understand data security issues and privacy solutions over SaaS.

Keywords: *Security, Security as a Service (SaaS), Security Assertion Markup Language (SAML), Secure Socket Layer (SSL),Transport Layer Security (TLS)*

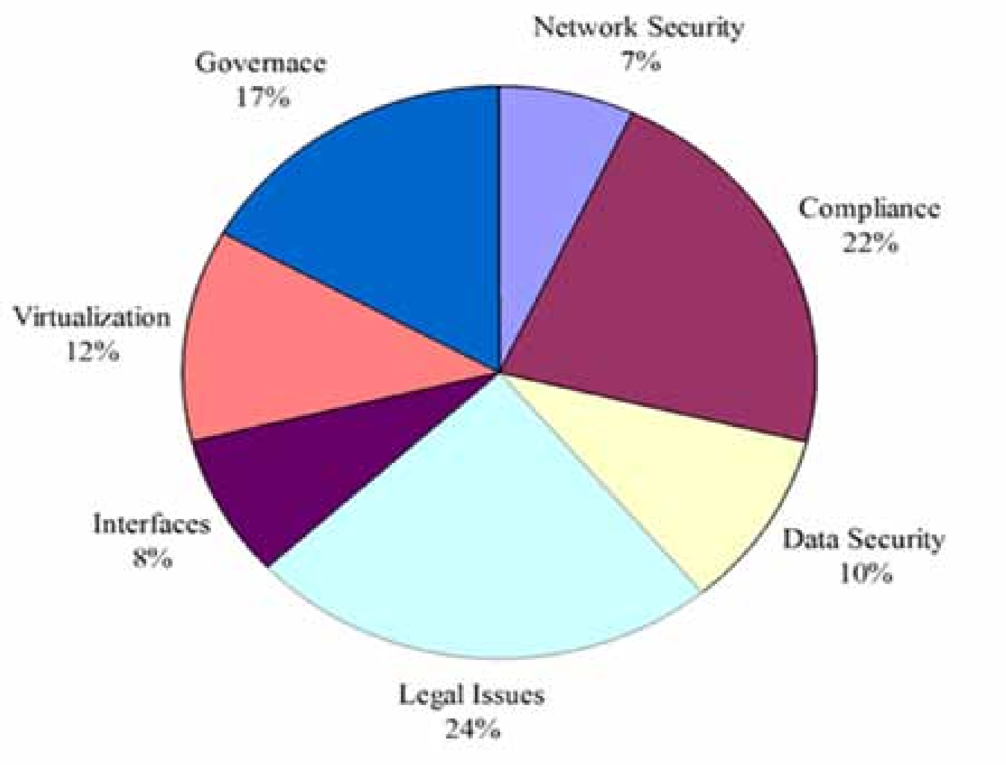
1. INTRODUCTION

In new computing paradigm cloud computing is most popular cost effective, flexible, highly available, pay per use computing web based service, which provides three service models (SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service)) four Deployment model (Private, Public, Hybrid, and Community) and five essential characteristics (On demand self service, Broad network access, Resource pooling, Rapid elasticity, Measured service) (Jansen, 2011; Paul, 2014; Tiwari, 2012).

Traditional storage, data management scheme is not superior enough to store and analyzing the big data. Cloud virtual information framework system has the capacity to handle the enormous information issue, yet it is insufficient great in security of information (Hassanien et al., 2015). Providers to ensure robust security system to users. Service providers used third party security and security audit systems. Service providers provide security, SecaaS (Security as a Service). SecaaS includes authentication, antivirus, anti malware, intrusion detection and security management at different level. SecaaS control the data loss

DOI: 10.4018/IJSSMET.2015070104

Figure 1. Security problems in grouped categories (Chen et al., 1994)



prevention, web security, encryption, network security and disaster recovery (Alliance, 2011b; Pearson, 2013).

Cloud Users can access computing resources via internet. Security is the main concern for cloud users. Security is dived mainly seven categories *(a) Legal issues (b) Network (c) Interface (d) Information (data security) (e) Compliance (f) Virtualization and (g) Governance* (Gonzalez et al., 2012).

The Result shows the legal issues and compliance are major security issues is shown in Figure 1. Pie chart shows virtualization has greater security vulnerabilities then network security. Virtualization gives the elasticity, resource pooling and multi tenancy facility in cloud computing (David, 2009; Luo, 2011).

Amazon AWS provides EC2 (Elastic Cloud Computing) and S3 (Simple Storage Service) with secure system. Amazon AWS uses multiple third party authorized audit security system (ISO/IES-27002 control frame work). Salesforce.com provides secure SaaS services with CRM (Customer Resource Management) features. HP, IBM, Google, Window Azure also gives security assurance to users (Amazon, 2014; Azure, 2014; Somorovsky et al., 2011).

Cloud providers take care on network security, IT system (system security), information (data security) and application security. Security responsibility ensures from client side and server side (Ma, 2012). Service provider provides several new security trends, but they are still not providing full robust security mechanism till now. Amazon AWS EC2 offers physical security, environmental security and virtualization security. Salesforce.com CRM (Customer Resource Management) offers security responsibilities in physical and environmental security control. Microsoft AZURE uses token based

Understanding the Characteristics of Early and Late Adopters of Technology: The Case of Mobile Money

Peter Tobbin and Joseph Adjei (2012). *International Journal of E-Services and Mobile Applications (pp. 37-54).*

www.igi-global.com/article/understanding-characteristics-early-late-adopters/66084?camid=4v1a

Transforming Healthcare through Entrepreneurial Innovations: An Institutional View

Arto Wallin (2017). *International Journal of E-Services and Mobile Applications (pp. 1-17).*

www.igi-global.com/article/transforming-healthcare-through-entrepreneurial-innovations/173033?camid=4v1a