Chapter 84
A Comprehensive Report on Security and Privacy Challenges in Software as a Service

Pradeep Kumar Tiwari
https://orcid.org/0000-0003-0387-9236
Manipal University Jaipur, India

Sandeep Joshi
School of Computing and IT, Manipal University Jaipur, India

ABSTRACT

Researchers have done tremendous works for data security, but a robust security mechanism is not available yet. Researchers are doing continuous work to build robust SaaS mechanism. SaaS has several security vulnerabilities. Data security is still the most important challenge to researcher and they can constantly do research to protect the data over the network but they are facing numerous technical challenges to completely secure the cloud network and cloud storage. This work would be helpful to understand data security and privacy problems. Researchers can find the new way to understand SaaS security vulnerabilities and currently available solutions.

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, A.E., Azar, A.T., Snasel,

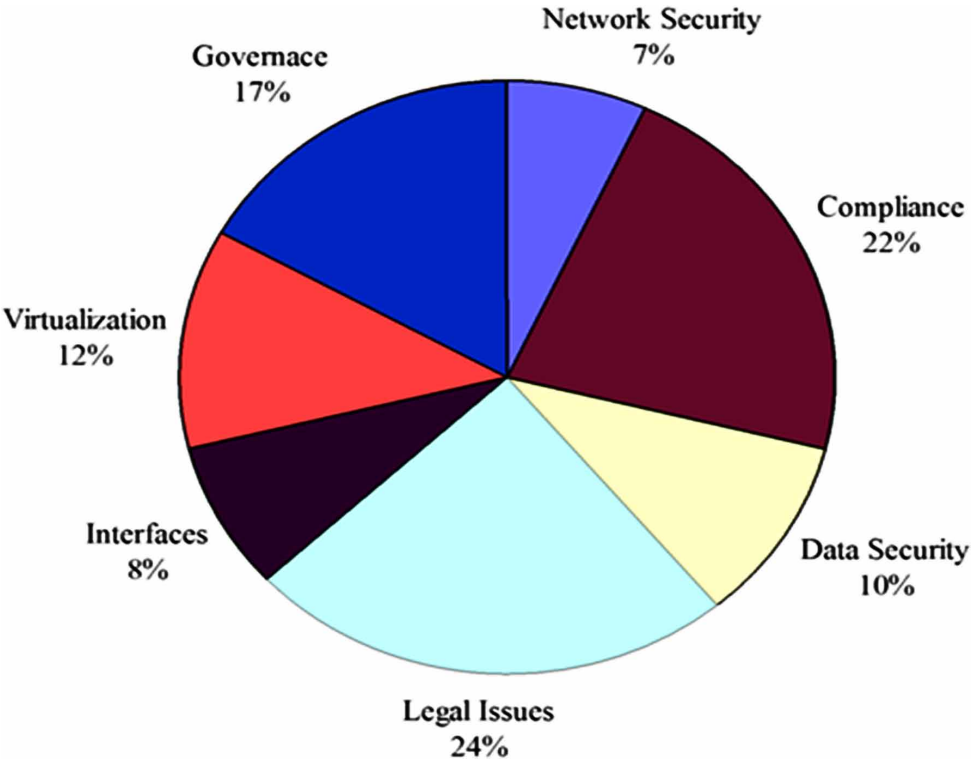
DOI: 10.4018/978-1-7998-5339-8.ch084

V., Kacprzyk, J., & Abawajy, J.H., 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 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: (1) Legal issues; (2) Network; (3) Interface; (4) Information (data security); (5) Compliance; (6) Virtualization and; (7) Governance (Gonzalez, N., Miers, C., Redígolo, F., Simplicio, M., Carvalho, T., Naslund, M., & Pourzandi, M., 2012).

The Result shows the legal issues and compliance are major security issues is shown in figure 1. Pi 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).

Figure 1. Security problems in grouped categories (Chen, P. M., Lee, E. K., Gibson, G. A., Katz, R. H., & Patterson, D. A., 1994)



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, J., Heiderich, M., Jensen, M., Schwenk, J., Gruschka, N., & Lo Iacono, L., 2011).