Computers and Electrical Engineering 71 (2018) 28–42

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Recent security challenges in cloud computing☆

Nalini Subramanian Research Scholar*, Andrews Jeyaraj

School of Computing, Sathyabama Institute of Science and Technology, Chennai, India

ARTICLE INFO

Keyword:
Security challenges
Cloud computing
Crypto-cloud
Issues in cloud
Virtualization

ABSTRACT

Cloud computing is an archetype that enables access to a shared pool of computing resources for cloud users in an on-demand or pay-per-use, fashion. Cloud computing offers several benefits to users and organizations, in terms of capital expenditure and savings in operational expenditure. Despite the existence of such benefits, there are some obstacles that place restrictions on the usage of cloud computing. Security is a major issue that is always considered. The lack of this vital feature results in the negative impact of the computing archetype thus resulting in personal, ethical, and financial harm. This paper will focus and explore the security challenges that are faced by cloud entities. These entities include Cloud Service Provider, the Data Owner and Cloud User. Focusing on the crypto-cloud that constitutes of different Communication, Computation, and Service Level Agreement. Studying the causes and effects of various cyber attacks it will provide the necessary upgrades.

1. Introduction

Cloud computing creates a network-based environment vision to the users, which paves way for the sharing of calculations and resources regardless of location. The National Institute of Standards and Technology's (NIST) defines cloud computing [1] as, “A template for providing the suitable and when needed access to the internet, to a collective pool of programmable grids, storage, servers, software, and amenities that can be rapidly emancipated, with little communication and supervision from the provider”. The characteristics of the type of processing are exhibited in Fig. 1 as On-demand self-service, High-performance network access, Rapid Elasticity, Resource Pooling and Measured Service. It also depicts four deployment models namely Hybrid, Community, Private and Public clouds. This is then coupled with the three service models, which are, PAAS (Platform as a Service), IAAS (Infrastructure as a Service), and SAAS (Software as a Service). NIST's cloud computing definition provides the needed framework and common characteristics depicted such as Virtualization, Homogeneity, Geographic Distribution and Service Orientation among others.

With all the layers of the cloud service models depicted in Fig. 2, security issues need to be addressed. When the layers are to be compared the high dependence of the browser position's it at the top whereas, the bottom layers are more web services oriented. Overall, a decrease in investment and operational expenses is achieved this is also followed by an increase in efficiency and scalability through the layers

The service model deployed can be private, public, hybrid or community cloud as per the user requirements.

Organization: The next two sections that follow indicate the security challenges. Sections 4–7 address the security challenges in communication, computational, data level and Service Level Agreement (SLA) level. Finally, Section 8, provides the conclusion with a comparison of the author's survey with other pre-existing reviews

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Associate Editor Dr. Hong Shen.

* Correspoding author.
E-mail addresses: mrgn.nalini@gmail.com (N. Subramanian), andrewspose@gmail.com (A. Jeyaraj).

https://doi.org/10.1016/j.compeleceng.2018.06.006
Received 8 July 2017; Received in revised form 13 June 2018; Accepted 29 June 2018

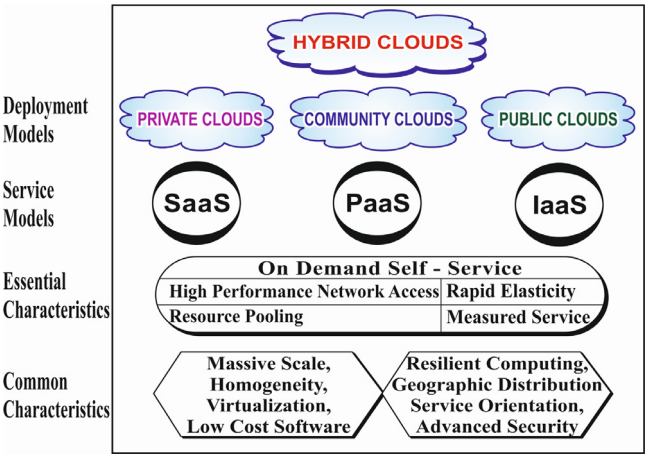

Fig. 1. NIST cloud definition framework.

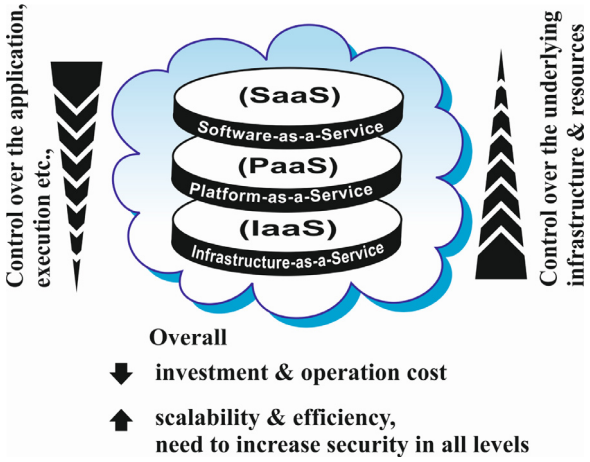

Fig. 2. Layers of cloud computing.

2. Security challenges

In cloud computing, the users are unaware of the exact location of their sensitive data, because the Cloud Service Providers(CSP's) maintain data centers in geographically distributed locations resulting in several security challenges and threats. The traditional security techniques such as firewalls, host-based antivirus software and intrusion detection systems do not offer adequate security in virtualized systems due to the rapid spread of the threats via virtualized environments.

2.1. Cloud computing threats and risks

On the other hand, Walker [2] identified that Cloud Security Alliance (CSA) has released the top 12 threats related to the cloud. These twelve threats are listed in Table 1. Among all these threats, data breaching is identified as the topmost security issue that needs addressing.

2.2. Security in crypto-cloud

Kamara [3], outlined the benefits of using a public cloud infrastructure. They also pointed out that the use of public clouds leads to several security risks. Confidentiality and integrity of the data are among the biggest risks causing grave concerns.

Fig. 3 clearly depicts the architecture of a crypto-cloud proposed by Kamara [3] in 2010. It consists of three basic entities, namely the Data Authority (the owner of the data), the consumer of the data, and the Cloud Storage Service Provider (CSSP). Data authority uploads the encrypted files, and the consumer or user of the cloud has authenticated access to the files. After these conditions are fulfilled then the requested file can be downloaded and decrypted using appropriate tokens and credentials. These entities face different security challenges in levels of communication, computation and Service Level Agreements (SLA's).