IMPACT: International Journal of Research in Engineering & Technology (IMPACT: IJRET)
ISSN (P): 2347-4599; ISSN (E): 2321-8843
Vol. 5, Issue 8, Aug 2017, 51-60
© Impact Journals

A QUANTITATIVE ANALYSIS OF SECURITY ISSUES IN CLOUD COMPUTING

JAYALAKSHMI K, UMA K M, VEENA A & LAVANYA SANTHOSH

Assistant Professor, Department of Computer Science and Engineering,

Dr. Ambedkar Institute of Technology, Bengaluru, India

ABSTRACT

In cloud computing technology, user can store large amount of data on storage provided by cloud and make use of resources as and when required, due to which, it becomes very significant. As a result, cloud computing technology has recently become a new model, by which we can host and deliver services over the internet. In cloud computing, resources are shared between different computers and other devices by means of the internet. There are so many issues, which have been observed in a cloud computing environment that need to be addressed. These issues can be categorized as: Security, Protection, Identity Management, Management of resources, Management of Power and Energy, Data Isolation, Availability of resources and Heterogeneity of resources. The first point of security, where, cryptography can facilitate cloud computing is secure storage, but the major disadvantages of secure storage is that we cannot perform processing on encrypted data. This paper presents the challenges and issues of security aspects in cloud computing method. We first look into the impacts of the distinctive characteristics of cloud computing, namely, multi-tenancy, elasticity and third party control, upon the security requirements. Then, we analyze the cloud security requirements in terms of the fundamental issues, i.e., confidentiality, integrity, availability, audit and compliance.

KEYWORDS: Availability, Cloud Computing, Cloud Security, Confidentiality, Elasticity, Integrity, Multi-Tenancy, Security