

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320-088X

IJCSMC, Vol. 2, Issue. 8, August 2013, pg.248 – 251

RESEARCH ARTICLE



SECURITY TECHNIQUES FOR MULTI TENANCY APPLICATIONS IN CLOUD

¹C.C. Kalyan Srinivas, Assistant Professor, Dept. of CSE, KMMITS, Tirupathi

²S.Sajida, Assistant Professor, Dept. of MCA, KMMIPS, Tirupathi

³Lokesh, M.Tech Student, KMMIPS, Tirupathi

Abstract: In cloud-based architectures, multi-tenancy means that customers, organizations, and consumers are sharing infrastructure and databases in order to gain price and performance advantages. At its simplest, the “cloud” is an Internet-based environment of computing resources comprised of servers, software, and applications that can be accessed by any individual or business with Internet connectivity. In the case of these “service” offerings, customers (or “tenants”) get a piece of the cloud that contains the resources they need to run their business. Cloud computing is the basis for infrastructure as a service (IaaS) and software as a service (SaaS). These services offer a pay-as-you-go lease style investment with little or no upfront costs versus buying all of the hardware and software outright. Other benefits include the ability to scale easily and tier more services and functionality on an “as needed” basis. The benefits, in fact, are so compelling that cloud computing is predicted by some to be the replacement for traditional means of obtaining these services and business capabilities by 2014. The big concern is how to ensure that proper security and isolation protects consumers or tenants of these services from the risks they pose to one another. Hence to provide security for various applications being run in multi tenancy, we are proposing a model based on segmentation on Hyper-visor, Database in the cloud.

Full Text: <http://www.ijcsmc.com/docs/papers/August2013/V2I8201341.pdf>