



CLOUD SECURITY AND COMPLIANCE - A SEMANTIC APPROACH IN END TO END SECURITY

R.Kalaiprasath ^{1*} R.Elankavi ¹ R.Udayakumar ³

¹Research Scholar, Bharath University, Chennai, Asst. Professor, Aksheyaa college of Engineering, Chennai.

³Associate Professor, Department of Information Technology, Bharath University, Chennai.

Email: koolkalai@gmail.com

Submitted: May 27, 2017

Accepted: June 15, 2017

Published: Sep 1, 2017

Abstract- The Cloud services are becoming an essential part of many organizations. Cloud providers have to adhere to security and privacy policies to ensure their users' data remains confidential and secure. Though there are some ongoing efforts on developing cloud security standards, most cloud providers are implementing a mish-mash of security and privacy controls. This has led to confusion among cloud consumers as to what security measures they should expect from the cloud services, and whether these measures would comply with their security and compliance requirements. We have conducted a comprehensive study to review the potential threats faced by cloud consumers and have determined the compliance models and security controls that should be in place to manage the risk. Based on this study, we have developed an ontology describing the cloud security controls, threats and compliances. We have also developed an application that classifies the security threats faced by cloud users and automatically determines the high level security and compliance policy controls that have to be activated for each threat. The application also displays existing cloud providers that support these security policies. Cloud consumers can use our system to formulate their security policies and find compliant providers even if they are not familiar with the underlying technology.

Index terms: Cloud computing, cloud security, Security compliance models, Cloud security models.