

**CHENNAI – PONDICHERRY**

**Assurance of Security and Privacy Requirements for Cloud Deployment Models**

**Abstract:**

Despite of the several benefits of migrating enterprise critical assets to the Cloud, there are challenges specifically related to security and privacy. It is important that Cloud Users understand their security and privacy needs, based on their specific context and select cloud model best fit to support these needs. The literature provides works that focus on discussing security and privacy issues for cloud systems but such works do not provide a detailed methodological approach to elicit security and privacy requirements neither methods to select cloud deployment models based on satisfaction of these requirements by Cloud Service Providers. This work advances the current state of the art towards this direction. In particular, we consider requirements engineering concepts to elicit and analyze security and privacy requirements and their associated mechanisms using a conceptual framework and a systematic process. The work introduces assurance as evidence for satisfying the security and privacy requirements in terms of completeness and reportable of security incident through audit. This allows perspective cloud users to define their assurance requirements so that appropriate cloud models can be selected for a given context. To demonstrate our work, we present results from a real case study based on the Greek National Gazette.

**Existing System:**

Security and privacy are major concerns for organiza-tions, which hinder cloud adaption as migrating into the cloud means organizations need to store their sensitive electronic assets into the providers’ infrastructure [18]. Existing business applications and data are mostly con-trolled through the provider’s infrastructure depending on the chosen model, i.e. Saas, PaaS, IaaS, on which users may not have full/any control. Users’ data are generally stored in a multi-tenant platform.

This scenario intro-duces extra security and privacy challenges comparing to the traditional computing environment. Lack of monitoring facility of user data incurs less user confidence on cloud based systems. Techniques to analyze the security and privacy issues in the context of cloud computing are different to those provided by the existing literature for traditional computing environments.

It is therefore necessary to develop methods that not only identify and analyse security and privacy requirements but also provide certain assurance that these require-ments are met by a specific cloud model before undertak-ing the migration decision. While such initiative have been put in place in for tradional IT based systems, the literature fails to provide evidence of a framework that fulfills that objective for cloud based services. This paper provides work towards this direction.

**Proposed System:**

The novelty of the proposed modeling language is the fact that it combines concepts from the requirements en-gineering, cloud computing, security, privacy and audit-ing domain. It uses new concepts such as cloud user, cloud service provider, audit, and mechanism, which are necessary to elicit and analysis of requirements and checks evidences to support these requirements based on organizational context. The metamodel of the language defines all concepts.

The central concept of the proposed language is that of an actor, which represents an entity that has strategic goals and intentions within a system or an organisational setting. An actor can be human, a system, or an or-ganisation. In our case, organization, cloud user and cloud service provider are three different types of actors. A cloud user actor can be individual or organization who needs cloud service and deployment model to support its specific strategic goal and intention. A cloud service pro-vider actor has two unique properties, i.e., service and deployment model to support the cloud users.