

**CHENNAI – PONDICHERRY**

**Risk-Aware Management of Virtual Resources in Access Controlled Service-oriented Cloud Datacenters**

**Abstract:**

For economic benefits and efficient management of resources, organizations are increasingly moving towards the paradigm of “cloud computing” by which they are allowed on-demand delivery of hardware, software and data as services. However, there are many security challenges which are particularly exacerbated by the multitenancy and virtualization features of cloud computing that allow sharing of resources among potentially untrusted tenants in access controlled cloud datacenters. This can result in increased risk of data leakage. To address this risk vulnerability, we propose an efficient risk-aware virtual resource assignment mechanism for clouds multitenant environment. In particular, we introduce the notion of sensitivity in datacenters and the objective is to minimize the risk of data leakage. In addition, the risk should not exceed in high sensitivity datacenters in comparison to low sensitivity datacenters. We present three assignment heuristics and compare their relative performance.

**Existing System:**

The security challenges in cloud computing present a major obstacle for adopting the cloud computing paradigm. The number of cloud security related incidents are on the rise. Cloud Security Alliance (CSA)1 identified the top security threats in cloud computing for as data breaches resulting from vulnerability of shared virtual resources. An example of data breach is the vulnerability of Google Docs where many documents are exposed to unauthorized users.

The cloud providers usually implement resource isolation mechanisms to counter the risk of data leakage and to increase the resource utilization at the same time. However, resource sharing remains the main security concern of cloud customers. Therefore, security-aware resource scheduling is needed in order to minimize the risk to which cloud customers application services are exposed in a multitenant cloud environment.

**Proposed System:**

We don’t consider container-based isolation because we assume that a VM can host only one service at a time as mentioned. The cloud architecture a depicts the other three types of isolations. In this paper, we do not address the problem of VM isolation. But rather, given the VM isolation techniques implemented by IaaS providers which can vary in their isolation guarantees, our objective is to manage the virtual resource, such that, if a vulnerability weakens the isolation among VMs, then the total risk of data leakage is minimized. If the VM isolation becomes stronger, the risk decreases but it does not vanish