

**CHENNAI – PONDICHERRY**

**Probabilistic Optimization of Resource Distribution and Encryption for Data Storage in the Cloud**

**Abstract:**

In this paper, we develop a decentralized probabilistic method for performance optimization of cloud services. We focus on Infrastructure-as-a-Service where the user is provided with the ability of configuring virtual resources on demand in order to satisfy specific computational requirements. This novel approach is strongly supported by a theoretical framework based on tail probabilities and sample complexity analysis. It allows not only the inclusion of performance metrics for the cloud but the incorporation of security metrics based on cryptographic algorithms for data storage. To the best of the authors’ knowledge this is the first unified approach to provision performance and security on demand subject to the Service Level Agreement between the client and the cloud service provider. The quality of the service is guaranteed given certain values of accuracy and confidence. We present some experimental results using the Amazon Web Services, Amazon Elastic Compute Cloud service to validate our probabilistic optimization method.

**Existing system:**

Approaches have been proposed to overcome this problem, commercial clouds have not been able to implement efficient systems where users pay for specific performance measures such as CPU and memory utilization rather than a flat hourly rate service. In commercial IaaS, such as the one provided by Amazon Web Services, Amazon Elastic Compute Cloud (AWS EC2), the set of possible configurations only allows for coarse-grained variations of the control inputs of the system. This imposes a challenge to apply performance regulation using existing techniques based on model identification and control systems theory.

**Proposed System:**

We present a mathematical decentralized approach to optimally distribute virtual resources in the cloud based on tail probabilities and sample complexity.

We consider a metric of encryption of stored data in the cloud along with other performance measures in the optimization problem.

We introduce a heuristic algorithm for the parallelization of the optimization process.

Propose quantitative methods to measure cloud security levels based on *Reference Evaluation Methodology* (REM) and *Quantitative Policy Trees* (QPT). REMand QPT allow the incorporation of security in the SLA along with other performance metrics associated with IaaS. In order to protect sensitive information stored in and traveling through the cloud, we propose the implementation of a variety of encryption ciphers according to the SLA to address current security issues associated with data storage.