

**CHENNAI – PONDICHERRY**

**CSR: Classified Source Routing in DHT-Based Networks**

**Abstract:**

In recent years cloud computing provides a new way to address the constraints of limited energy, capabilities, and resources. Distributed hash table (DHT) based networks have become increasingly important for efficient communication in large-scale cloud systems. Previous studies mainly focus on improving the performance such as latency, scalability and robustness, but seldom consider the security demands on the routing paths, for example, bypassing untrusted intermediate nodes. Inspired by Internet source routing, in which the source nodes specify the routing paths taken by their packets, this paper presents CSR, a tag-based, Classified Source Routing scheme in DHT-based cloud networks to satisfy the security demands on the routing paths. Different from Internet source routing which requires some map of the overall network, CSR operates in a distributed manner where nodes with certain security level are tagged with a label and routing messages requiring that level of security are forwarded only to the qualified next-hops. We show how this can be achieved efficiently, by simple extensions of the traditional routing structures, and safely, so that the routing is uniformly convergent. The effectiveness of our proposals is demonstrated through theoretical analysis and extensive simulations.

**Existing System:**

Internet source routing, in which source nodes partially or fully specify the paths taken by their packets, is a fundamental means of providing path diversity to improve Internet communications. Inspired by Internet source routing, we consider improving cloud routing from the applications’ perspective, i.e., allowing source nodes to specify their desired routing paths in the networks where there exist multiple paths between any pairs of nodes. Despite the flexibility obtained by source nodes, however, the characteristics of cloud networks such as large scale and dynamic stabilization, make it difficult to realize the application specified routing.

**Proposed System:**

We focus on (i) how to efficiently maintain tags in the routing tables, and (ii) how to effectively satisfy the tagged requirements (i.e., security levels) of messages during the routing. We do not study how to decide the security levels for different servers which should be addressed by application-specific methods orthogonal to CSR, or how to construct the trust model for detection of malicious nodes which has been widely studied in the literature and we assume that there already has been a security hierarchy (e.g., a company’s administrative structure).