Reputation-Based Security System For Edge Computing

Abstract

Given the centralized architecture of cloud computing, there is a genuine concern about its ability to adequately cope with the demands of connecting devices which are sharply increasing in number and capacity. This has led to the emergence of edge computing technologies, including but not limited to mobile edge-clouds. As a branch of Peer-to-Peer (P2P) networks, mobile edge-clouds inherits disturbing security concerns which have not been adequately addressed in previous methods. P2P security systems have featured many trust-based methods owing to their suitability and cost advantage, but these approaches still lack in a number of ways. They mostly focus on protecting client nodes from malicious service providers, but downplay the security of service provider nodes, thereby creating potential loopholes for bandwidth attack. Similarly, trust bootstrapping is often via default scores, or based on heuristics that does not reflect the identity of a newcomer. This work has patched these inherent loopholes and improved fairness among participating peers. The use cases of mobile edge-clouds have been particularly considered and a scalable reputation based security mechanism was derived to suit them. BitTorrent protocol was modified to form a suitable test bed, using Peersim simulator. The proposed method was compared to some related methods in the literature through detailed simulations. Results show that the new method can foster trust and significantly improve network security, in comparison to previous similar systems.

composability Compositionality Computing Theory and Trust mobile edge-clouds p2p pubcrawl reputation resilience Resiliency Scalability Security Heuristics trust