ABSTRACT

Social IoT (SIoT) is an architectural pattern for IoT, which involves IoT devices with social, behavioural attributes. A key challenge in implementing a SIoT-based service network in a multi-vendor environment of heterogeneous devices is Trust. We propose a hybrid trust management framework that uses Probabilistic Neighbourhood Overlap, a graph-based concept that is fundamental to our model. Our proposed trust management framework makes use of both human intelligence and device (artificial) intelligence for trust management. Also, the framework uses a mix of dynamic (interaction-based) and static (graph-based) approaches, balancing between system resource requirements and trust assessment accuracy. We demonstrate the resilience of our framework to various security attacks via theoretical and simulation-based analysis, using real-world datasets.