

Sicherheit in der Transportschicht für die Kommunikation vom Internet der Dinge zu Cloud-Servern

Ein Heimenergie-Management-System (HEMS) kann die Elektrizitätskosten eines Haushalts minimieren, indem es Preisdaten nutzt, um Geräte zu steuern. Diese Kommunikationen können mit einer Publizier/Abonnier-Architektur abgebildet werden, die von MQTT, einem Protokoll auf Anwendungsebene für das Internet der Dinge (IoT) implementiert wird. Im Gegensatz dazu sind übliche Protokolle in den meisten Fällen Anfrage/Antwort-basiert. Die Sicherheitsanforderungen der Kommunikationen können mit TLS adressiert werden.

Diese Arbeit schlägt MQTT gesichert mit TLS für die Kommunikation eines HEMS vor. Die Netzwerk-Performance von MQTT wird in reinen Bedingungen für zwei Phasen gemessen: Für den Verbindungsbeginn werden die Metriken Startzeit, übertragene Datenmenge und Rechenaufwand quantifiziert. Die Metriken für die bereits verbundene Phase sind Latenz, Durchsatz und Overhead. Schließlich werden MQTT und TLS für die Implementierung eines HEMS bewertet.