**MQTT (Message Queuing Telemetry Transport)**

Protokol MQTT  adalah protokol komunikasi yang digunakan untuk pertukaran data ringan antara perangkat dalam jaringan IoT (Internet of Things).  
Kelebihan

* Terbaik untuk aplikasi berdaya rendah
* Ideal untuk perangkat seluler bertenaga baterai
* Keandalan tinggi dalam menyampaikan pesan
* Dukungan untuk Koneksi yang Tidak Stabil
* Sumber daya CPU minimal
* Opsi kualitas layanan (QoS) yang fleksibel
* Protokol standar OASIS

Kontra

* Umumnya tidak cocok untuk aplikasi perangkat lunak konsumen
* Kurangnya enkripsi
* Dukungan keamanan minimal (dapat mengurangi risiko dengan bekerja sama dengan penyedia keamanan)
* Kecepatan yang relatif rendah
* Tidak ada kemampuan panggilan video
* Kompleksitas Konfigurasi: Konfigurasi dan manajemen broker MQTT dapat menjadi rumit terutama dalam skala besar. Pemantauan dan skalabilitas mungkin memerlukan penanganan tambahan.

**WebSocket**

WebSocket dapat berfungsi sebagai landasan bagi aplikasi pesan instan berskala besar. WebSocket adalah WebSocket adalah protokol komunikasi yang menyediakan saluran komunikasi penuh-duplex (full-duplex) melalui satu sambungan TCP tunggal. Ini memungkinkan klien dan server untuk berkomunikasi secara dua arah dengan cara yang lebih efisien daripada protokol HTTP tradisional.

Kelebihan

* Fungsionalitas obrolan waktu nyata
* Memperbarui antarmuka dengan data baru secara otomatis
* Komunikasi dua arah lebih cepat dibandingkan HTTP dan AJAX
* Kompatibel antara platform web, desktop, dan seluler
* Hanya memiliki biaya overhead 2 byte

Kontra

* Keandalan dibatasi oleh koneksi internet pengguna
* Membutuhkan browser web yang sepenuhnya mendukung HTML5
* Tidak menyediakan cache perantara/tepi
* Tidak dapat menggunakan status HTTP ramah dan elemen lainnya
* Lebih sulit untuk dikembangkan daripada HTTP
* Firewall dan Proxy: Beberapa firewall dan proxy mungkin tidak sepenuhnya mendukung WebSocket, yang dapat menyulitkan implementasi di beberapa lingkungan jaringan.
* Kekhawatiran Keamanan: Koneksi WebSocket yang tetap terbuka dapat meningkatkan risiko serangan seperti serangan DoS (Denial of Service) atau serangan peretasan.

**XMPP (Extensible Messaging and Presence Protocol)**

XMPPsebuah protokol terbuka yang digunakan untuk komunikasi real-time seperti obrolan (chat), kolaborasi, dan transfer data antara berbagai sistem yang berbeda.

Kelebihan

* Mendukung panggilan suara, panggilan video, dan transfer file
* Desain yang dapat diperpanjang
* Fleksibilitas sumber terbuka
* Menggunakan protokol komunikasi internet standar (ICP)
* Berkomunikasi melalui HTTP
* Stabilitas dan keandalan
* Arsitektur terdesentralisasi
* Dapat mengisolasi di jaringan pribadi untuk keamanan tambahan
* Prinsip Desentralisasi: XMPP beroperasi berdasarkan prinsip desentralisasi, yang berarti setiap organisasi atau entitas dapat mengoperasikan server XMPP-nya sendiri. Hal ini memberikan kontrol lebih besar kepada pengguna atas data dan privasi mereka.

Kontra

* Tidak memiliki dukungan QoS
* Tidak efektif dalam mengirimkan data biner
* Tidak ada enkripsi ujung ke ujung
* Relatif lambat