تکنولوژی جدید(HTTP3) موجب ارسال سریع‌تر داده می‌شود، آسیب‌پذیری کمتری از جهت خطاها دارد و تأخیر کاهش پیدا می‌کند تا شروع بارگذاری اطلاعات از سرورها، زودتر اتفاق بیافتد. HTTP3 به صورت پیش‌فرض رمزگذاری دارد و لذا نیازی به استفاده کردن از روش‌های رمزگذاری مجزا نیست. در این نسخه از الگوریتم TLS نسخه‌ی 1.3 برای رمزگذاری استفاده می‌شود که در واقع در HTTPS فعلی هم کاربرد دارد.

یک تفاوت اساسی بین HTTP2 و HTTP3 در نحوه‌ی ارسال بسته‌های داده بر بستر اینترنت است. در پروتکل جدید به جای استفاده از **TCP** از **UDP** استفاده می‌شود. هر دو پروتکل TCP و UDP برای ارسال بیت‌های داده در شبکه به کار می‌روند اما در روش TCP که قدیمی‌تر است، بسته‌های داده به صورت **مرتب** و **توأم با چک کردن خطاها** ارسال می‌شود و روشی **قابل اعتماد** است. اما مشکل این است که اگر حتی یک بسته‌ی داده در فرآیند ارسال، به دلیلی از بین برود و به مقصد نرسد، تمام فرآیند با مشکل مواجه می‌شود.

HTTP3 بر اساس QUIC یا Quick UDP Internet Connections طراحی شده و از پروتکل UDP برای ارسال داده استفاده می‌کند. در این روش، **ترتیب** و **چک کردن خطا** وجود ندارد و لذا مثل TCP قابل اعتماد نیست اما در مقابل این مزیت را دارد که سریع‌تر است. اگر بسته‌ی از داده از دست برود، اپلیکیشن دریافت‌کننده‌ی داده‌ها می‌تواند آن را مجدداً درخواست کند و البته این درخواست می‌تواند با استفاده از پروتکل TCP انجام بشود که قابل اطمینان است.

بنابراین در HTTP3 داده‌ای که از بین رفته، فقط داده‌های مربوط به همان بسته را تحت تأثیر قرار می‌دهد و ارسال سایر بسته‌ها متوقف نمی‌شود.