

Arsitektur Jaringan Peer-to-Peer untuk Aplikasi Kolaboratif Aman dalam Waktu Nyata Berbasis IPFS = Peer-to-Peer Network Architecture for Secure Collaborative Applications in Real-Time Based on IPFS

Walangadi, Dennis Al Baihaqi, author

Deskripsi Lengkap: <https://lib.ui.ac.id/detail?id=9999920542497&lokasi=lokal>

Abstrak

Aplikasi kolaboratif adalah jenis perangkat lunak yang dirancang untuk memfasilitasi kerja sama dan komunikasi antara pengguna secara daring. Umumnya, aplikasi kolaboratif dirancang dengan menggunakan arsitektur yang terpusat. Namun, arsitektur ini memiliki beberapa isu seperti rentan terhadap penyensoran dan menjadi titik tunggal terjadinya serangan yang bisa berakibat pada kebocoran data pengguna. Arsitektur peer-to-peer bisa menjadi solusi untuk isu tersebut. Implementasi arsitektur peer-to-peer perlu memenuhi kebutuhan menyimpan dan memuat data pengguna tanpa adanya otoritas terpusat. IPFS bisa menjadi salah satu alternatif untuk menyimpan data pengguna secara terdistribusi. Namun, data yang disimpan di IPFS bersifat publik sehingga memerlukan adanya lapisan keamanan untuk menjaga kerahasiaan data yang disimpan. Dilatarbelakangi oleh permasalahan tersebut, penelitian ini memperkenalkan sebuah arsitektur terdistribusi yang aman berbasis IPFS. Terdapat 3 aspek yang dievaluasi yaitu aspek latensi pada waktu nyata, aspek kinerja transfer data pada tempat penyimpanan, dan aspek kerahasiaan pada saat sesi kolaborasi serta pada data yang diunggah ke IPFS. Penelitian ini menemukan bahwa implementasi WebRTC berbasis IPFS memiliki kinerja latensi yang lebih baik apabila dibandingkan dengan arsitektur terpusat. Selain itu, dalam arsitektur peer-to-peer, algoritma CRDT dibuktikan mampu untuk menangani resolusi konflik pada sebuah sesi kolaborasi dengan banyak peer. Penelitian ini juga menunjukkan bahwa IPFS mampu mendukung kebutuhan aplikasi kolaboratif untuk menyimpan, memuat, dan berbagi dokumen secara peer-to-peer. Kinerja transfer data pada IPFS cenderung lebih baik daripada solusi terpusat, baik dengan jumlah data yang berbeda maupun jumlah node yang terhubung. Selain itu, penggunaan enkripsi mampu menjaga aspek kerahasiaan data yang diunggah ke IPFS. Selain itu, UUID sebagai identitas sebuah ruangan dalam aplikasi kolaboratif mampu memberikan lapisan kerahasiaan untuk pengguna aplikasi.

.....Collaborative apps are a type of software designed to facilitate cooperation and communication between users online. Generally, collaborative applications are designed using a centralized architecture. However, this architecture has several issues such as being vulnerable to censorship and being a single point of attack that can result in the leakage of user data. Peer-to-peer architecture can be a solution to these issues. The implementation of peer-to-peer architecture needs to meet the needs of storing and loading user data without a centralized authority. IPFS can be one of the alternatives to store user data in a distributed manner. However, the data stored in IPFS is public so it requires a security layer to maintain the confidentiality of the stored data. Against this background, this research introduces a secure distributed architecture based on IPFS. There are 3 aspects evaluated, namely the latency aspect in real time, the data transfer performance aspect on the storage, and the confidentiality aspect during collaboration sessions as well as on data uploaded to IPFS. This research found that IPFS-based WebRTC implementation has better latency performance when compared to centralized architecture. In addition, in a peer-to-peer architecture, the CRDT algorithm is proven to be able to handle conflict resolution in a collaboration session with

multiple peers. This research also shows that IPFS is able to support the needs of collaborative applications to store, load, and share documents on a peer-to-peer basis. Data transfer performance on IPFS tends to be better than centralized solutions, both with different amounts of data and the number of connected nodes. In addition, the use of encryption is able to maintain the confidentiality aspect of the data uploaded to IPFS. In addition, UUID as the identity of a room in a collaborative application is able to provide a layer of confidentiality for application users.