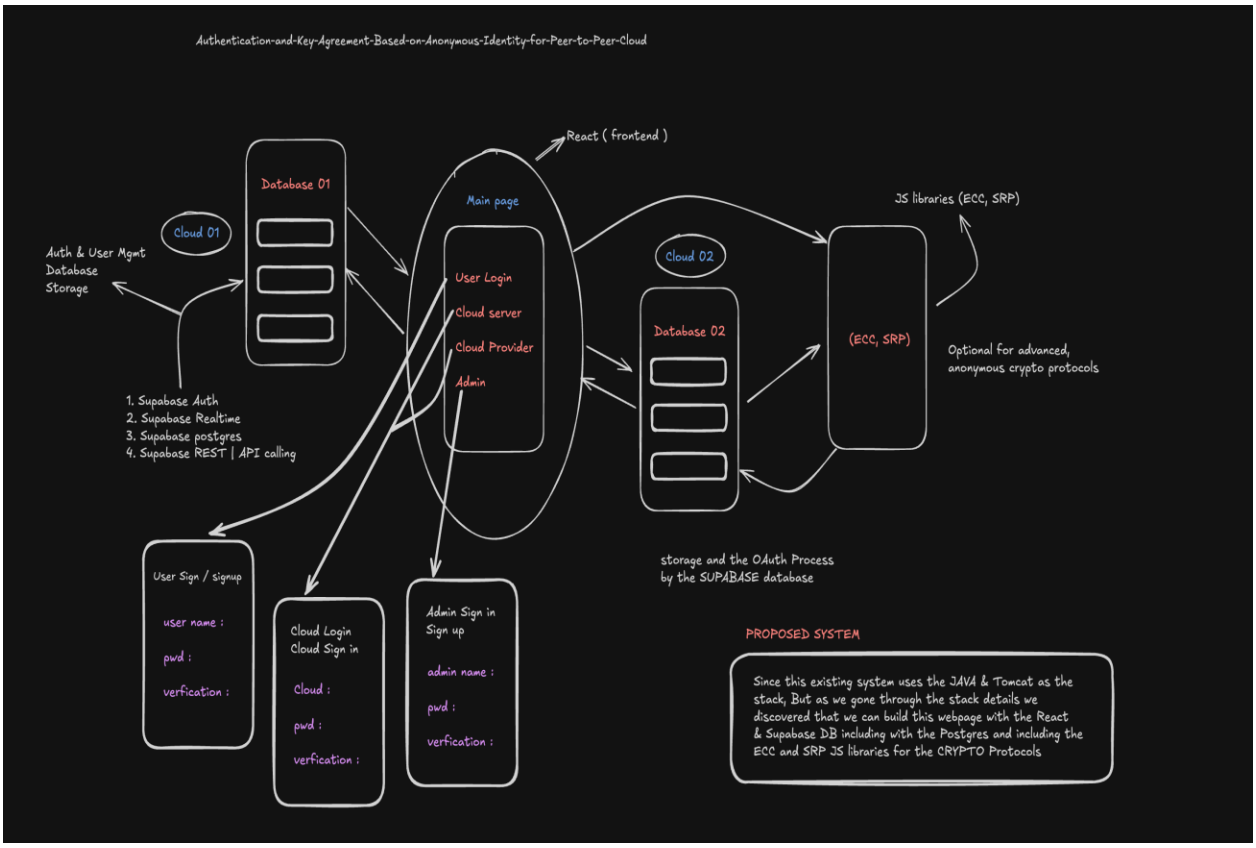
ABSTRACT

This proposed system presents a secure and privacy-preserving authentication and key agreement framework designed for Peer-to-Peer (P2P) cloud environments using anonymous identities. The architecture leverages advanced cryptographic techniques including Elliptic Curve Cryptography (ECC), Secure Remote Password (SRP) protocols, and zero-knowledge proofs to ensure mutual authentication and confidential session key establishment without revealing participants' real identities. By removing reliance on centralized trusted authorities and utilizing decentralized P2P frameworks like libp2p, the system supports scalable, robust, and efficient data migration and communication across cloud boundaries. The integration of modern frontend technologies such as React, combined with Supabase's backend-as-a-service platform offering PostgreSQL database, authentication, and real-time capabilities, enables rapid development and deployment with seamless user identity management and secure coordination. The solution balances anonymity and traceability, ensuring accountability when needed while preserving user privacy. Overall, this system offers a modern, scalable, and practical approach to secure anonymous authentication and key agreement suitable for evolving decentralized cloud applications.



1. https://jespublication.com/upload/2022-V13I7149.pdf
2. https://ijsrst.com/home/issue/view/article.php?id=IJSRST219193
3. https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-023-00446-2
4. https://www.ijraset.com/research-paper/substantiation-and-key-agreement-based-on-unidentified-identity-for-peer-to-peer-cloud
5. https://www.ijarst.com/article/348
6. http://www.journal-iiie-india.com/1_sep_23/1_online.pdf