PROJECT TITLE:

AUTHENTICATION & KEY AGREEMENT BASED ON ANONYMOUS IDENTITY FOR PEER-TO-PEER CLOUD

Abstract:

Peer-to-peer (P2P) cloud systems offer scalability and decentralization but face challenges in secure and private communication. This work presents a lightweight authentication and key agreement protocol using anonymous identities and elliptic curve cryptography (ECC). The scheme enables mutual authentication and secure session key establishment without revealing real identities, ensuring confidentiality, integrity, and resistance to replay, impersonation, and man-in-the-middle attacks. Its efficiency makes it suitable for dynamic, resource-constrained P2P cloud environments, enhancing both privacy and trustworthiness in distributed data sharing.

Keywords:

Peer-to-Peer (P2P) Cloud, Authentication, Key Agreement, Anonymous Identity, Elliptic Curve Cryptography (ECC), Privacy

Technologies used:

Python, MySQL, Socket Programming (Comm), Elliptic Curve Cryptography (ECC), Diffie–Hellman Algorithm, Anonymous Identity-based Authentication

22R01A7332- I.YASHWANTH

22R01A7335- K. RISHI ROHAN

22R01A7348 – N.M.A.K. NAVEEN

Signature of the Guide   **Signature of the Project Coordinator**

K. Vinay Kumar   **C. Vijay Kumar**