IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, June 2025
Impact Factor: 7.67

Ensuring Secure Sharing of Identity Information of KYC Compliance and Verification

J. Dinesh[1], N. Vignesh[2], Mohd Firasat Ali[3], Mr. G. Mukesh[4]
B.Tech Student, Cyber Security Department[1,2,3]
Assistant Professor, Cyber Security Department[4]
Sphoorthy Engineering College, Hyderabad

Abstract: *The increasing dependence on centralized servers for storing around 70% of user data, including sensitive details such as addresses, zip codes, gender, and medical history, presents serious risks of misuse or unauthorized alterations. To counter these threats, a Blockchain-based KYC Sharing system is introduced, utilizing Blockchain's robust features of encryption, access control, and immutability. Each record is stored as a transaction or block, linked to a unique HASHCODE that ensures data integrity by verifying all previous HASHCODEs before adding new information. Users retain explicit control over data access, and whenever an organization retrieves their KYC details, Blockchain automatically sends an email notification, enhancing transparency and accountability. Additionally, Smart Contracts written in Solidity optimize the storage and retrieval process within the Blockchain. This system strengthens secure data sharing, minimizes privacy breaches, and fosters a more user-focused and trustworthy approach to data management, addressing key concerns of centralized storage.*

Keywords: centralized servers, sensitive information, KYC, Blockchain, data encryption, access control, immutability, HASHCODE

DOI: 10.48175/IJARSCT-27614