Notification:F.no.COE/Ph.D/(Notification/571/2024)

Name of research Scholar: Saba Khanum

Name of Supervisor: Prof. Khurram Mustafa

Name of department: Computer Science Department

Title of P.hD. Thesis: Sensitive Data Protection on Blockchain Applications.

Keywords: Cryptocurrency,Sensitive data,Blockchain, Protection **,**Security.

Findings

Blockchain application security focuses on a comprehensive risk management strategy designed to address vulnerabilities within blockchain networks. This strategy incorporates cybersecurity frameworks, assurance services, and industry best practices to reduce risks related to attacks and fraud. However, the transparency of blockchain leads to privacy issues, as transaction details are publicly available, allowing easy identification of users through network analysis. This raises concerns among financial institutions, hindering the widespread use of blockchain. Sensitive data, such as personal and financial information, must be securely stored, and access should be limited to authorized users. This study, conducted using the PRISMA systematic review method, examines how sensitive data flows through blockchain applications and identifies key vulnerabilities in blockchain wallets and transactions. The findings highlight the need for improved security measures to protect sensitive data. The study also addresses the increasing threats of social engineering, ransomware, and advanced persistent threats (APTs) in the blockchain space, which pose significant risks. A proposed solution includes generating an automatic key for heirs in the event of the wallet owner's death, using Elliptic Curve Diffie-Hellman and Blind Signatures for secure key exchange. Additionally, an affordable hardware wallet and an Android app are suggested to ensure offline key storage and transaction privacy. Finally, the research introduces a Zero-Knowledge Proof-based validation system and Lattice-Based Blind Ring Signature encryption to enhance blockchain security.