Privacy Preserving Password Manager with Zero-Knowledge Proof Authentication

Sushant Ambastha
Students, Department of Computer Applications & Technology (SCAT), Galgotias University, Greater Noida, Uttar Pradesh, India

Abhishek Bajetha
Students, Department of Computer Applications & Technology (SCAT), Galgotias University, Greater Noida, Uttar Pradesh, India

Abhijit Kumar
Students, Department of Computer Applications & Technology (SCAT), Galgotias University, Greater Noida, Uttar Pradesh, India

Dr. Neetu Sharma
Professor, Department of Computer Applications & Technology (SCAT), Galgotias University, Greater Noida, Uttar Pradesh, India

Abstract:

Password managers serve an essential function in contemporary digital networks because they protect user passwords across different websites. The centralized storage and trust-based authentication methods that traditional systems use create security weaknesses which lead to data breaches and privacy violations. ZKPass delivers a password management solution which protects user privacy through its implementation of Zero-Knowledge Proof (ZKP) protocols that eliminate the requirement for servers and verifiers to access user passwords. Users can demonstrate their identity through this system which protects all of their personal data while keeping their authentication process secure. ZKPass protects local password storage through complete end-to-end encryption while using cryptographic elements to stop unauthorized access during server breaches. The proposed architecture minimizes attack surfaces through its implementation of secure key derivation and hash-based commitment schemes and session-based proof verification[1]. The user credential management system provides enhanced security features while giving users complete authority over their credential information. The experimental tests show that the system provides strong authentication security while consuming very little processing power. The foundation of ZKPass establishes Next Generation password management systems which combine user-friendly design and high operational efficiency and strong privacy protection through Zero-Knowledge authentication [2].

Keywords:

Zero-Knowledge Proof, Password Manager, SRP Protocol, Cryptography, End-to-End Encryption, Authentication.