

ABSTRAK

MUH. AL IQRAM MARZAH, Implementasi Sistem *Dekripsi* Token Untuk Mencegah Berbagi Akun Pada Aplikasi Guru Pintar di Sekolah. (dibimbing oleh Rizki Yuslana Bakti, S.T.,M.T, dan Muhyiddin AM Hayat, S.Kom.,M.T).

Penelitian ini bertujuan untuk mengimplementasikan sistem dekripsi token berbasis perangkat (*device-bound token decryption*) pada aplikasi *Guru Pintar* untuk mencegah praktik berbagi akun. Aplikasi *Guru Pintar* hadir sebagai solusi digital dalam mendukung pembelajaran, namun menghadapi permasalahan serius terkait keamanan, khususnya risiko kebocoran data akibat penggunaan akun secara bersamaan di perangkat berbeda. Sebagai solusi inovatif, sistem yang dikembangkan dirancang dengan framework Electron dan memanfaatkan *device fingerprinting* untuk mengikat token autentikasi pada identitas perangkat keras tertentu. Data penelitian diperoleh melalui proses implementasi dan diuji menggunakan metode *black box testing* dengan berbagai skenario login. Hasil pengujian menunjukkan bahwa sistem mampu menolak login dari perangkat yang berbeda meskipun kredensial valid, serta terbukti aman terhadap serangan umum seperti *SQL injection*, *XSS*, dan *token tampering*. Temuan ini menunjukkan bahwa penerapan dekripsi token berbasis perangkat efektif dalam meningkatkan keamanan autentikasi, menjaga keunikan akses pengguna, dan memperkuat perlindungan data pada aplikasi edukasi digital.

Kata Kunci : *dekripsi token*, keamanan akun, *device-bound token*, *device fingerprinting*, berbagi akun, *Electron JS*.

ABSTRAK

MUH. AL IQRAM MARZAH, *Implementation of a Token Decryption System to Prevent Account Sharing in the Guru Pintar Application in Schools.* (supervised by Rizki Yusliana Bakti, S.T., M.T., and Muhyiddin AM Hayat, S.Kom., M.T.).

This research aims to implement a device-bound token decryption system in the Guru Pintar application to prevent account sharing. The Guru Pintar application is presented as a digital solution to support learning, but faces serious security issues, particularly the risk of data leakage due to concurrent account use on different devices. As an innovative solution, the developed system is designed with the Electron framework and utilizes device fingerprinting to bind authentication tokens to specific hardware identities. Research data was obtained through the implementation process and tested using black box testing methods with various login scenarios. The test results show that the system is able to reject logins from different devices even though the credentials are valid, and is proven secure against common attacks such as SQL injection, XSS, and token tampering. These findings indicate that the implementation of device-based token decryption is effective in improving authentication security, maintaining the uniqueness of user access, and strengthening data protection in digital education applications.

Keywords: *token decryption, account security, device-bound token, device fingerprinting, account sharing, Electron JS.*