INTISARI

Keamanan data sensitif merupakan aspek penting dalam pengembangan aplikasi layanan publik berbasis *mobile*. Aplikasi Dolan Banyumas sebagai aplikasi pariwisata daerah mengelola data pengguna yang bersifat sensitif, seperti informasi identitas dan data akun, sehingga memerlukan mekanisme pengamanan yang memadai. Pada sistem awal, pengamanan data masih terbatas pada penggunaan *hashing MD5* untuk *password*, sementara data sensitif lainnya belum mendapatkan perlindungan yang optimal.

Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem keamanan data menggunakan pendekatan kriptografi hibrid pada aplikasi Dolan Banyumas. Pendekatan kriptografi hibrid dilakukan dengan mengombinasikan algoritma *AES-256-GCM* sebagai algoritma kriptografi simetris untuk mengenkripsi data sensitif pengguna dan algoritma *RSA-2048* sebagai algoritma kriptografi asimetris untuk mengamankan kunci enkripsi *AES*. Sementara itu, mekanisme *hashing MD5* tetap digunakan untuk pengamanan *password* pengguna.

Metode penelitian yang digunakan meliputi tahap analisis sistem, perancangan sistem keamanan, implementasi, serta pengujian sistem. Pengujian sistem dilakukan melalui pengujian fungsional menggunakan metode *blackbox testing*, pengujian keamanan meliputi pengujian *SQL Injection* dan *brute force* menggunakan *Burp Suite* serta pengujian *sniffing* data menggunakan *Wireshark*, dan pengujian performa untuk mengukur kecepatan proses enkripsi dan dekripsi serta penggunaan penyimpanan data. Sistem diimplementasikan pada aplikasi *mobile* berbasis *Android* dengan server *backend* berbasis *PHP* dan basis data *PostgreSQL*.

Hasil penelitian menunjukkan bahwa penerapan kriptografi hibrid mampu meningkatkan keamanan data sensitif pengguna pada aplikasi Dolan Banyumas. Data sensitif berhasil dilindungi baik saat proses pengiriman maupun saat penyimpanan, sistem memiliki ketahanan terhadap berbagai serangan keamanan, serta tidak mengalami penurunan performa yang signifikan. Dengan demikian, sistem keamanan yang diusulkan dinilai efektif dan layak diterapkan pada aplikasi layanan publik berbasis *mobile.*

Kata kunci: Kriptografi Hibrid, *AES-256-GCM*, *RSA-2048*, Keamanan Data, Dolan Banyumas

ABSTRACT

Data security is an essential aspect in the development of mobile-based public service applications. The Dolan Banyumas application, as a regional tourism application, manages sensitive user data such as identity information and account data, which requires adequate security mechanisms. In the initial system, data protection was limited to the use of MD5 hashing for passwords, while other sensitive data had not been optimally secured.

This research aims to design and implement a data security system using a hybrid cryptography approach in the Dolan Banyumas application. The hybrid cryptography approach combines AES-256-GCM as a symmetric cryptographic algorithm to encrypt sensitive user data and RSA-2048 as an asymmetric cryptographic algorithm to secure the AES encryption key. Meanwhile, MD5 hashing is still used to protect user passwords.

The research methodology includes system analysis, security system design, implementation, and system testing. System testing consists of functional testing using the black box testing method, security testing including SQL Injection and brute force testing using Burp Suite as well as data sniffing testing using Wireshark, and performance testing to measure encryption and decryption speed as well as data storage usage. The system is implemented on an Android-based mobile application with a PHP-based backend server and a PostgreSQL database.

The results show that the implementation of hybrid cryptography is able to enhance the security of sensitive user data in the Dolan Banyumas application. Sensitive data is successfully protected during data transmission and storage, the system demonstrates resistance to various security attacks, and no significant performance degradation is observed. Therefore, the proposed security system is considered effective and suitable for implementation in mobile-based public service applications.

Keyword: Hybrid Cryptography, AES-256, RSA-2048, Data Security, Dolan Banyumas