RINGKASAN

Prototype Sistem Keamanan File SKM (Surat Keterangan Medis) Pasien Menggunakan Algoritma AES di Rumah Sakit Bethesda Yogyakarta, Olivia Christiany Putri, NIM G41230678, Tahun 2026, Manajemen Informasi Kesehatan, Politeknik Negeri Jember, Donny Setiawan H.P. S,Kep., Ns., M.Kes (Dosen Pembimbing), Agung Dwi Saputro, S.KM., MARS (Clinical Instructure).

Perkembangan digitalisasi dalam pelayanan kesehatan meningkatkan kebutuhan terhadap keamanan dan kerahasiaan informasi pasien, termasuk file surat menyurat pasien yang dikelola pada bagian Surat Keterangan Medis (SKM) Rumah Sakit Bethesda Yogyakarta. Berdasarkan hasil observasi, file surat menyurat pasien dibuat menggunakan template Microsoft Word dan disimpan dalam folder berdasarkan nama pasien. File juga dapat dikirimkan secara elektronik kepada pemohon melalui WhatsApp, sehingga diperlukan perlindungan tambahan untuk menjaga kerahasiaan file dari akses pihak yang tidak berwenang. Oleh karena itu, kegiatan ini bertujuan untuk mengidentifikasi kondisi keamanan dan kerahasiaan file surat menyurat pasien, mengidentifikasi kebutuhan keamanan dalam proses penyimpanan dan pengiriman secara elektronik, merancang prototipe sistem keamanan menggunakan algoritma Advanced Encryption Standard (AES), serta mengimplementasikan AES untuk proses enkripsi dan dekripsi file.

Metode yang digunakan dalam kegiatan ini adalah metode informasi teknologi dengan sumber data yang diperoleh melalui observasi dan dokumentasi pada bagian SKM Rumah Sakit Bethesda Yogyakarta. Observasi dilakukan untuk mengetahui proses pembuatan, penyimpanan, dan pengiriman file surat menyurat pasien serta kondisi keamanan dan kerahasiaannya. Berdasarkan hasil identifikasi tersebut, dirancang prototipe SIPAS-AES (Sistem Pengamanan Arsip Surat Menggunakan Algoritma AES) sebagai aplikasi desktop menggunakan rancangan antarmuka yang

dibuat dengan Figma. Prototipe menyediakan fitur pemilihan file melalui tombol dan *drag and drop*, pilihan proses enkripsi dan dekripsi, input password, serta notifikasi hasil proses. Format file yang dirancang untuk didukung meliputi PDF, JPG, PNG, dan DOCX.

Hasil kegiatan menunjukkan bahwa prototipe SIPAS-AES telah dirancang dan diimplementasikan menggunakan algoritma AES dengan mode *Galois/Counter Mode* (GCM). Proses enkripsi menghasilkan file berekstensi .enc, sedangkan proses dekripsi mengembalikan file ke bentuk semula menggunakan password yang sesuai. Prototipe juga dilengkapi validasi input dan notifikasi keberhasilan maupun kegagalan proses. SIPAS-AES diharapkan dapat menjadi alternatif pengamanan tambahan bagi file surat menyurat pasien dalam penyimpanan dan pengiriman elektronik. Pengembangan selanjutnya dapat mempertimbangkan fitur dekripsi melalui aplikasi mobile Bethesda untuk mempermudah akses dokumen oleh pasien atau pihak yang berwenang.