ABSTRAK

Rekam medis elektronik (*Electronic Medical Records*/EMR) menyimpan informasi penting mengenai kondisi pasien dan memerlukan perlindungan yang kuat terhadap risiko manipulasi atau perubahan data tidak sah (*tampering*). Penelitian ini bertujuan untuk merancang dan mengevaluasi sistem penyimpanan rekam medis berbasis *private blockchain* yang difokuskan pada peningkatan integritas dan keaslian data medis. Sistem dirancang menggunakan kombinasi algoritma *hashing* SHA-256, tanda tangan digital ECDSA, serta enkripsi AES, dengan mekanisme konsensus *Proof of Authority* (PoA) untuk validasi blok.

Rancangan sistem mencakup autentikasi pengguna berbasis peran, otorisasi eksplisit oleh pasien, validasi transaksi, pembentukan blok, serta sinkronisasi dan resolusi konflik antar-*node*. Pengujian dilakukan pada prototipe berskala terbatas dengan mensimulasikan berbagai bentuk *tampering*, termasuk perubahan *hash*, prev_hash, *signature*, dan isi transaksi.

Hasil pengujian menunjukkan bahwa sistem mampu mendeteksi dan menolak setiap manipulasi yang dilakukan pada data maupun blok. Proses otorisasi pasien terbukti efektif dalam memastikan data tidak dapat dipublikasikan tanpa persetujuan pemiliknya, sementara mekanisme validator berhasil menjaga konsistensi rantai blok. Dengan demikian, penelitian ini membuktikan bahwa penerapan *private blockchain* dapat meningkatkan perlindungan terhadap *tampering* dan menjaga integritas rekam medis elektronik, meskipun aspek skalabilitas, interoperabilitas, dan performa jaringan besar masih menjadi ruang pengembangan lanjutan.

Kata Kunci: *Private Blockchain*, *Tampering*, Integritas Data, Tanda Tangan Digital, *Hashing*