BAB 1
PENDAHULUAN

1.1. Latar Belakang

Adopsi teknologi *Blockchain* dalam sistem pencatatan kesehatan elektronik (*Electronic Health Records*/EHR) terus meningkat karena sifatnya yang terdesentralisasi, transparan, dan tidak dapat diubah, sehingga mampu menjamin integritas serta keaslian data pasien secara lebih efektif dibanding sistem konvensional [1][2][3]. Meskipun demikian, beberapa studi terdahulu menunjukkan bahwa penerapan blockchain di bidang kesehatan masih menghadapi tantangan besar dalam aspek keamanan dan privasi, terutama dalam mencegah akses tidak sah dan menjaga kerahasiaan data sensitif [4][5]. Oleh karena itu, dibutuhkan algoritma kriptografi yang kuat, efisien, dan tahan terhadap berbagai jenis serangan**,** guna mendukung sistem EHR berbasis *Blockchain* yang andal dan aman [6].

Menjawab tantangan tersebut, banyak sistem blockchain saat ini mengandalkan algoritma *Elliptic Curve Digital Signature Algorithm* (ECDSA) karena kemampuannya menghasilkan tanda tangan digital yang ringkas namun tetap kuat dari sisi keamanan melalui pendekatan *Elliptic Curve Discrete Logarithm Problem* [7][8]. Namun, efisiensi algoritma ini masih menjadi sorotan karena proses matematis seperti *modular inversion* dan *scalar multiplication* yang kompleks dapat menyebabkan penurunan kinerja, terutama saat digunakan pada sistem berskala besar seperti EHR [9]. Lebih lanjut, penelitian juga menunjukkan bahwa ECDSA rentan terhadap kesalahan implementasi, misalnya pada penggunaan *Random Number Generator* (RNG) yang lemah, yang berpotensi membuka celah keamanan kritis pada data kesehatan yang seharusnya dilindungi.

Sebagai respons terhadap keterbatasan ECDSA, algoritma *Edwards-curve Digital Signature Algorithm* (EdDSA) dikembangkan untuk memberikan solusi yang lebih efisien tanpa mengorbankan keamanan. EdDSA menggunakan kurva *Twisted Edwards*, *nonce* deterministik, serta proses verifikasi yang lebih cepat, sehingga sangat cocok untuk implementasi pada sistem berbasis blockchain yang memerlukan kecepatan tinggi dan konsumsi sumber daya rendah [10]. Dalam

studi mereka, EdDSA terbukti mengungguli ECDSA dalam hal performa, khususnya dalam konteks *Blockchain* dan IoT. Bahkan, menurut publikasi oleh Wiley, EdDSA dinilai sebagai alternatif efisien dan terjangkau dari ECDSA, meskipun verifikasi tanda tangannya sedikit lebih berat dari sisi komputasi [11]. Dengan mempertimbangkan potensi tersebut, maka penting dilakukan komparasi menyeluruh antara ECDSA dan EdDSA dalam konteks keamanan catatan kesehatan berbasis *Blockchain* untuk menentukan algoritma yang paling sesuai dengan kebutuhan sistem EHR modern.

1.2. Rumusan Masalah

Rumusan masalah pada penelitian ini yaitu bagaimana perbandingan keamanan serta efektivitas dan efisiensi performa antara algoritma ECDSA dan EdDSA dalam melindungi integritas dan kerahasiaan sistem *Electronic Health Record* (EHR) berbasis *Blockchain*.

1.3. Batasan Masalah

Batasan masalah pada penelitian ini yaitu:

1. Dataset yang digunakan pada penelitian ini berupa *Electronic Health Record* (EHR) *dataset* yang diambil dari Kaggle.
2. Penelitian ini tidak mencakup pengembangan aplikasi blockchain lengkap, melainkan fokus pada simulasi dan evaluasi algoritma tanda tangan digital dalam konteks EHR.
3. *Output* hasil komparasi pada penelitian ini terdiri dari pengujian keamanan dan pengujian performa.

1.4. Tujuan Penelitian

Tujuan yang diharapkan dari penelitian ini yaitu:

1. Untuk mengetahui perbandingan keamanan antara algoritma ECDSA dan EdDSA dalam melindungi integritas dan kerahasiaan EHR berbasis *Blockchain*.
2. Untuk menganalisis efektivitas dan efisiensi performa algoritma ECDSA dan EdDSA dalam implementasi sistem EHR berbasis *Blockchain*.

1.5. Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini yaitu:

1. Manfaat Teoritis

   Penelitian ini dapat memperkaya kajian ilmiah di bidang kriptografi dan keamanan sistem berbasis *Blockchain*, khususnya dalam penerapan algoritma tanda tangan digital pada sistem *Electronic Health Record* (EHR). Hasil komparasi antara ECDSA dan EdDSA dapat menjadi referensi untuk penelitian lanjutan dalam memilih algoritma yang lebih efisien dan aman pada aplikasi yang memerlukan integritas serta privasi tinggi.

2. Manfaat Praktis

   Penelitian ini dapat memberikan wawasan bagi pengembang sistem informasi kesehatan dan praktisi keamanan data dalam memilih algoritma tanda tangan digital yang tepat, efisien, dan aman untuk sistem berbasis *Blockchain*. Hasil analisis performa dan keamanan yang disajikan diharapkan mampu mendukung pengambilan keputusan dalam desain arsitektur sistem EHR yang lebih handal.

3. Manfaat Akademik

   Penelitian ini dapat menjadi bahan referensi akademik bagi mahasiswa, dosen, dan peneliti yang tertarik dalam topik keamanan *Blockchain*, algoritma kriptografi modern, dan penerapannya pada sistem informasi kesehatan.

1.6. Keterbaruan Penelitian

Berikut ini akan diuraikan keterbaruan dari penelitian ini melalui *literature review* penelitian terdahulu yang berkaitan dengan topik penelitian antara lain:

1. Guruprakash Jayabalasamy & Srinivas Koppu membandingkan ECDSA dan EdDSA dalam domain Blockchain dan IoT. Hasilnya menunjukkan EdDSA secara signifikan lebih unggul dalam performa (waktu penandatanganan dan verifikasi), sambil tetap menjaga tingkat keamanan yang sama [11].
2. Penelitian yang dilakukan oleh Andi, et al., (2022) membahas mengenai penggunaan algoritma tanda tangan digital ECDSA dalam rangka memperkuat keamanan catatan medis pasien COVID-19 yang disimpan di

dalam sistem berbasis *Blockchain*. Hasil penelitian menunjukkan bahwa kombinasi ECDSA dan *Blockchain* mampu menjaga integritas, autentikasi, dan keamanan catatan medis pasien COVID-19, dengan mencegah akses tidak sah serta memastikan data tidak dapat dimanipulasi setelah tersimpan [7]**.**

3. Sebuah artikel di *ITM Conferences* (IWADI 2024) yang dipublikasikan oleh membahas perbandingan performa ECDSA dan EdDSA dalam skala luas, menunjukkan EdDSA unggul dalam operasi penandatanganan dan verifikasi, terlebih saat digunakan dalam aplikasi seperti EHR dan IoT [12].

Keterbaruan dari penelitian ini terletak pada perbandingan empiris langsung antara algoritma ECDSA dan EdDSA dalam konteks Blockchain dan EHR menggunakan dataset nyata, dengan analisis mendalam terhadap keamanan nonce deterministik EdDSA, evaluasi performa pada arsitektur skala besar, serta integrasi aspek teknis algoritma tanda tangan digital ke dalam studi sistem kesehatan terdistribusi, yang belum banyak dijelajahi dalam penelitian sebelumnya.