BAB I
PENDAHULUAN

1.1 Latar Belakang

Pertumbuhan e-commerce di Indonesia mengalami peningkatan yang pesat dan menjadi bagian penting dari ekonomi digital. Nilai transaksi yang terus bertambah menunjukkan adanya perubahan perilaku konsumen dan pola pasar. Namun, peningkatan jumlah transaksi ini juga diikuti oleh meningkatnya risiko keamanan siber dan kerentanan data internal[1]. Dalam konteks operasional *e-commerce*, permasalahan utama yang dihadapi tidak lagi terbatas pada ketersediaan layanan, tetapi telah bergeser pada bagaimana menjaga integritas dan transparansi data transaksi, khususnya pada proses *order* dan status pengiriman[2].

Dalam konteks operasional *e-commerce*, isu utama yang dihadapi tidak lagi terbatas pada ketersediaan layanan, tetapi telah bergeser pada urgensi menjaga integritas data transaksi. Dalam kerangka keamanan informasi CIA Triad (*Confidentiality, Integrity, Availability*), aspek Integritas didefinisikan sebagai jaminan bahwa data tidak dimodifikasi oleh pihak yang tidak berwenang (Chai & Zolkipli, 2021). Lebih mendalam, Warkentin dan Orgeron (2020) menegaskan bahwa tantangan terbesar dalam sistem *database* konvensional adalah kurangnya jaminan *non-repudiation* (ketidaksangkalan), yang menciptakan celah bagi pihak internal untuk memanipulasi riwayat data tanpa terdeteksi. Oleh karena itu, kebutuhan akan transparansi data yang dapat diaudit, khususnya pada proses pesanan dan status pengiriman, menjadi sangat krusial[3][4].

Kerentanan ini diperkuat oleh temuan dalam manajemen rantai pasok, yang mengidentifikasi bahwa proses pelacakan pesanan masih sangat rentan akibat penggunaan sistem informasi yang beragam, input manual, dan praktik operasional yang tidak konsisten. Sistem terpusat konvensional tidak hanya menderita masalah data manipulasi dan kegagalan titik tunggal, tetapi juga menghalangi transparansi sejati dalam operasi *e-commerce*[5]. Dalam konteks ini, teknologi blockchain dengan mekanisme hash chaining dan algoritma SHA-256 terbukti mampu

mengatasi kerentanan tersebut dengan menjamin *immutability* dan *traceability* data pengiriman melalui penciptaan audit trail yang transparan dan tidak dapat diubah.

Penelitian Veronica Martinez, Michael Zhao, Ciprian Blujdea, Xia Han, Andy Neely, dan Pavel Albores menunjukkan bahwa pengelolaan status pesanan dalam rantai pasok modern masih rentan akibat penggunaan berbagai sistem informasi, input manual, dan rendahnya *traceability*, sehingga diperlukan mekanisme kriptografi berbasis blockchain untuk menjamin *immutability* dan *traceability* data pengiriman[6]. Sejalan dengan itu membuktikan bahwa adopsi teknologi blockchain memberikan dampak signifikan terhadap kepercayaan konsumen dan perlindungan privasi, di mana penerapannya terutama ketika biaya operasional rendah atau kekhawatiran privasi tinggi mampu menghasilkan *win win outcome* bagi supplier, platform, dan konsumen, sekaligus memperkuat nilai dan keamanan dalam ekosistem e-commerce[7].

Solusi yang diusulkan adalah penerapan hash chaining pada lingkungan database terpusat, di mana setiap perubahan status pengiriman direpresentasikan sebagai blok yang memuat *hash* kriptografis dari status sebelumnya. Jika ada upaya manipulasi status historis, *avalanche effect* dari SHA-256 akan menyebabkan *mismatch hash*, sehingga sistem secara otomatis mengindikasikan ketidakkonsistenan dan membatalkan validitas rantai[8]. Dengan mekanisme ini, audit trail yang transparan dan *immutable* dapat terjamin tanpa ketergantungan pada blockchain publik yang kompleks.

Penelitian ini bertujuan untuk meningkatkan keamanan pada proses perubahan status pengiriman dalam sistem e-commerce. Algoritma SHA-256 dan konsep hash chaining digunakan untuk mencatat setiap pembaruan status sebagai jejak audit yang sulit diubah. Pendekatan ini dipilih karena lebih sederhana dan efisien dibandingkan penerapan blockchain secara penuh yang membutuhkan infrastruktur terdesentralisasi dan pengelolaan yang kompleks. Dengan pendekatan tersebut, prinsip *immutability* dan *traceability* dapat diterapkan secara lebih ringan dan mudah diintegrasikan pada sistem e-commerce skala menengah.

1.2 Rumusan Masalah

Dalam upaya memastikan integritas data dan mendeteksi manipulasi status pengiriman pada *platform e-commerce* BelanjaTech yang dikembangkan, penelitian ini berfokus pada dua permasalahan utama sebagai berikut:

1. Bagaimana mengimplementasikan mekanisme blockchain melalui struktur data hash chain berbasis SHA-256 untuk menjamin sifat immutability pada riwayat status pengiriman BelanjaTech?
2. Bagaimana merancang mekanisme *audit trail* yang mampu mendeteksi manipulasi data secara *real-time* melalui validasi hash pada setiap tahapan perubahan status pengiriman?

1.3 Batasan Masalah

Dalam penelitian ini, beberapa batasan ditetapkan untuk memperjelas ruang lingkup dan memastikan fokus kajian tetap terarah:

1. Penelitian berfokus berfokus pada perancangan dan implementasi logika keamanan data berbasis mekanisme *hash chaining* di sisi *backend* server. Platform *e-commerce* BelanjaTech yang dibangun menggunakan Next.js hanya berfungsi sebagai lingkungan uji untuk memvalidasi algoritma yang diterapkan, bukan sebagai produk akhir komersial.
2. Penelitian ini mengadopsi konsep struktur data berantai dalam lingkungan basis data terpusat menggunakan PostgreSQL dan Prisma ORM. Sistem tidak menerapkan teknologi *blockchain* yang dikendalikan oleh satu pihak atau satu server pusat yang melibatkan jaringan terpisah, melainkan menjamin integritas data secara internal pada server tunggal.
3. Sistem dirancang untuk interaksi antara dua entitas utama, yaitu Admin Toko sebagai pemicu update status pesanan dan Sistem/Superadmin sebagai pihak yang melakukan validasi serta penyimpan hash.
4. Pengamanan data menggunakan algoritma SHA-256 untuk proses hashing data transaksi yang mencakup status pesanan, *timestamp*, dan *previous hash*,

dengan mekanisme *hash chaining* di mana setiap hash baru dihitung berdasarkan kombinasi data saat ini dan hash sebelumnya.

5. Data yang diteliti berfokus pada status pesanan dan audit trail, tidak mencakup aspek keamanan *payment gateway* eksternal atau logistik fisik barang secara mendalam.
6. Sistem difokuskan secara spesifik pada kemampuan mendeteksi perubahan data manipulasi pada database melalui verifikasi integritas rantai hash. Ketika seorang penyerang atau *insider attack* mencoba mengubah data status pengiriman, sistem akan otomatis terdeteksi perubahan atau *data mismatch*.
7. Penelitian ini menerapkan konsep *blockchain* secara terintegrasi pada website *e-commerce* BelanjaTech, bukan sebagai *blockchain* terdesentralisasi yang berjalan pada jaringan *node* terpisah. Pencatatan block dilakukan pada database terpusat, dimana setiap perubahan status pengiriman disusun secara berurutan dan saling terhubung melalui nilai hash.
8. Penelitian ini tidak membahas aspek *User Interface/User Experience* (UI/UX) secara mendalam. Tampilan *website* dikembangkan sebatas purwarupa fungsional untuk memvisualisasikan data *audit trail* dan mempermudah proses pengujian *backend*.

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk mencapai beberapa tujuan utama terkait implementasi *blockchain* sebagai *audit trail* status pengiriman pada sistem *e-commerce:*

1. Merancang dan membangun logika *backend* pada platform BelanjaTech menggunakan arsitektur *server* terpusat menggunakan Next.js dan PostgreSQL yang menerapkan algoritma kriptografi SHA-256 dengan metode *hash chaining* untuk mengamankan riwayat status pesanan.

2. Mewujudkan sistem pencatatan data status pengiriman yang memiliki sifat mudah dideteksi jika diubah, sehingga setiap perubahan status pada pengiriman terekam secara urut, terhubung, dan tidak dapat dimanipulasi tanpa merusak rantai hash validasi.
3. Mengembangkan fitur verifikasi otomatis pada system BelanjaTech yang mampu mendeteksi kegagalan integritas data dan *data mismatch* apabila terjadi upaya pengubahan data secara ilegal langsung melalui database termasuk serangan oleh *insider*.
4. Mendemonstrasikan bahwa prinsip keamanan *immutable ledger* milik blockchain dapat diadopsi ke dalam sistem database relasional konvensional menggunakan PostgreSQL dan Prisma untuk kasus penggunaan e-commerce tanpa memerlukan infrastruktur desentralisasi yang kompleks.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan kontribusi signifikan baik secara teoritis maupun praktis dalam bidang keamanan sistem informasi dan *e-commerce*:

1. Manfaat Teoritis
   a. Memperkaya literatur mengenai implementasi mekanisme *hash chaining* menggunakan prinsip dasar *blockchain* dalam arsitektur basis data terpusat, sebagai alternatif solusi integritas data yang efisien tanpa memerlukan kompleksitas infrastruktur *blockchain* terdesentralisasi.
   b. Menjadi rujukan akademis bagi peneliti selanjutnya dalam mengembangkan model deteksi manipulasi data menggunakan algoritma kriptografi SHA-256 pada sistem informasi berbasis web modern.
2. Manfaat Praktis
   a. Menyediakan mekanisme keamanan tambahan yang mampu mencegah *insider attack* dan manipulasi data oleh pihak internal, serta menyediakan fitur *audit trail* otomatis yang tidak dapat diubah, sehingga

mencegah manipulasi status pesanan secara diam-diam oleh administrator basis data.

b. Memberikan bukti digital yang sah dan dapat diverifikasi melalui fitur lencana keamanan ("Verified"), yang berfungsi sebagai instrumen validasi bagi pengguna untuk memastikan bahwa riwayat transaksi mereka adalah otentik dan belum dimodifikasi
c. Meningkatkan kepercayaan terhadap *platform e-commerce* BelanjaTech karena adanya jaminan transparansi jejak pesanan yang dapat diverifikasi integritasnya sehingga dapat meminimalisir potensi sengketa transaksi di kemudian hari.

1.6 Sistematika Penulisan

Untuk mempermudah pemahaman dalam penyusunan skripsi ini, sistematika penulisan disusun sebagai berikut:

1. **BAB I PENDAHULUAN**

   Bab ini menguraikan latar belakang masalah mengenai kerentanan manipulasi data transaksi oleh pihak internal (*insider threat*) pada sistem *e-commerce*. Bab ini juga memaparkan rumusan masalah, batasan masalah yang berfokus pada implementasi *hash chaining* di sisi *backend*, tujuan penelitian, manfaat penelitian, serta sistematika penulisan laporan.

2. **BAB II TINJAUAN PUSTAKA**

   Bab ini memuat kajian literatur mengenai konsep keamanan data, ancaman *insider attack*, dan teknologi *blockchain*. Bab ini juga membahas landasan teori pendukung seperti algoritma kriptografi SHA-256, mekanisme *Hash Chaining*, arsitektur REST API, kerangka kerja Next.js, serta metode pengujian *Black Box Testing* yang digunakan sebagai dasar pengembangan sistem.

3. **BAB III METODOLOGI PENELITIAN**

   Bab ini menjelaskan tahapan penelitian secara sistematis, dimulai dari analisis kebutuhan sistem, perancangan arsitektur *backend* BelanjaTech, hingga desain basis data PostgreSQL yang menerapkan skema tabel *ledger*

(*OrderBlock*). Bab ini juga menjabarkan alur logika algoritma penguncian data, spesifikasi perangkat keras/lunak, serta skenario pengujian keamanan yang akan dilakukan.

4. **BAB IV HASIL DAN PEMBAHASAN**

   Bab ini merupakan inti penelitian yang memaparkan hasil implementasi sistem, mulai dari struktur basis data, antarmuka pengguna (*Store Dashboard*, *My Orders*) dan antarmuka pengawasan website e-commerce untuk *Superadmin*/Sistem, hingga logika *hashing* pada API. Bab ini juga menyajikan hasil pengujian sistem menggunakan metode *Black Box Testing* untuk membuktikan keberhasilan fitur deteksi manipulasi data (*Tamper Detection*) dalam skenario serangan basis data langsung.

5. **BAB V PENUTUP**

   Bab ini berisi kesimpulan dari seluruh rangkaian penelitian, yang menegaskan efektivitas algoritma SHA-256 dalam menjamin integritas *audit trail*. Bab ini diakhiri dengan saran untuk pengembangan sistem lebih lanjut, seperti penerapan desentralisasi server dan mekanisme notifikasi keamanan otomatis.