BAB I Pendahuluan

1.1.Latar Belakang Masalah

Deteksi penipuan merupakan bidang penting dalam riset dan aplikasi industri karena sifat penipuan yang merugikan dan sulit diidentifikasi. Teknik statistik dan *rule-based* telah digunakan untuk menemukan ketidakteraturan data. Namun, pendekatan ini memiliki keterbatasan, terutama dalam menghadapi skala data modern dan pola penipuan yang terus berevolusi [1].

Penipuan pada e-commerce berkembang lebih kompleks, tidak lagi terkait dengan transaksi tunggal, melainkan muncul dari interaksi antara perangkat, identitas, alat pembayaran, dan pola perilaku temporal. Berdasarkan survei Q1 2025 Digital Trust Index yang dilakukan Sift terhadap 1.075 responden dewasa di Amerika Serikat, 44% konsumen pernah menjadi korban penipuan pembayaran sepanjang hidupnya dan 62% pernah membatalkan transaksi online karena kekhawatiran terhadap keamanan [2]. *Card-not-present* (CNP) merupakan ancaman yang semakin meningkat pesat dalam *e-commerce* [3].

CNP merupakan bentuk penipuan yang terjadi pada transaksi daring tanpa kehadiran fisik kartu, dan terus meningkat seiring pertumbuhan e-commerce serta evolusi taktik pelaku penipuan. Laporan industri menunjukkan bahwa kerugian akibat penipuan pembayaran online mencapai puluhan miliar dolar per tahun dan diproyeksikan terus meningkat, dengan dampak tidak langsung berupa biaya tambahan, kenaikan harga, dan penurunan kepercayaan konsumen

CNP mencakup berbagai modus penipuan, seperti *carding attacks* yang memanfaatkan data kartu hasil kebocoran, *first-party fraud* melalui penyalahgunaan mekanisme chargeback, serta phishing, pengambilalihan akun, dan skema triangulasi yang melibatkan penggunaan identitas dan informasi pembayaran pihak lain [3]. Modus-modus ini menunjukkan bahwa CNP tidak hanya bergantung pada satu transaksi ilegal, tetapi sering kali muncul dari penyalahgunaan atribut identitas, pola perilaku, dan urutan aktivitas yang tampak sah.

Anonimitas transaksi digital dan minimnya verifikasi fisik menjadikan CNP sulit dideteksi, karena aktivitas penipuan dapat menyerupai perilaku pengguna normal. Dalam beberapa kasus, bahkan terjadi kolusi antara pelaku penipuan dan konsumen yang secara sadar terlibat dalam transaksi ilegal. Kondisi ini menegaskan bahwa deteksi CNP memerlukan pendekatan yang mampu melakukan profiling lintas entitas dan memodelkan dinamika perilaku transaksi dari waktu ke waktu, bukan sekadar analisis transaksi individual.

Salah satu strategi melawan penipuan adalah memanfaatkan *machine learning* yang mampu menganalisis data dalam skala besar dan mendeteksi pola mencurigakan secara langsung [3]. Namun demikian, pendekatan machine learning konvensional umumnya beroperasi pada representasi fitur yang bersifat statis tanpa melibatkan dinamika perilaku yang berkembang dari waktu ke waktu [4].

Pendekatan berbasis *Deep Learning* seperti *Convolutional Neural Networks* (CNN) terbukti dapat menemukan pola tabular [5]. CNN sendiri menghadapi tantangan signifikan karena model hanya menangkap pola statis dengan syarat interaksi lokal.

Gated Recurrent Unit (GRU) dirancang khusus untuk memproses data sekuensial dengan kemampuan mempertahankan memori jangka panjang secara efektif. GRU mampu mengatur aliran informasi secara selektif dan menentukan data mana yang harus disimpan atau dilupakan sehingga ideal untuk mendeteksi perubahan pola atau perilaku dinamis dari waktu ke waktu, sesuai dengan kebutuhan analisis pola sekuensial di transaksi. Dibandingkan dengan arsitektur *Long Short-Term Memory* (LSTM), GRU menawarkan struktur yang lebih sederhana dan efisiensi komputasi yang lebih tinggi, memungkinkan proses pelatihan yang lebih cepat tanpa mengorbankan akurasi dalam menangkap ketergantungan temporal.

Meskipun penelitian sebelumnya menunjukkan efektivitas CNN dan GRU, masih terbatas penelitian *hybrid* yang secara eksplisit menekankan keseimbangan antara performa prediktif dan efisiensi operasional pada kondisi *real-time*.

Oleh karena itu penelitian ini bertujuan menerapkan sebuah model *deep learning hybrid* ringan untuk deteksi penipuan. Model ini mengintegrasikan 2 komponen inti: (1) CNN untuk menangkap interaksi fitur yang terlokalisasi dalam data tabel terstruktur, dan (2) GRU untuk memodelkan dependensi temporal di dalam perilaku transaksi yang berlangsung secara berurutan. Dengan mengombinasikan kedua pendekatan tersebut, model *hybrid* mampu mempelajari pola dari fitur statis dan temporal, mengatasi keterbatasan masing-masing pendekatan tunggal. Arsitektur yang diusulkan diharapkan memiliki efisiensi komputasi yang lebih baik serta kemudahan implementasi di lingkungan nyata.

1.2.Rumusan Masalah

1. Bagaimana merancang dan mengimplementasikan model *hybrid deep learning* menggunakan CNN dan GRU untuk mendeteksi penipuan dalam sebuah data transaksi *e-commerce*?
2. Seberapa akurat dan efisienkah model deteksi penipuan *hybrid* CNN-GRU ketika diterapkan pada data transaksi *e-commerce*?

1.3.Batasan Masalah

Penelitian ini memiliki batasan masalah untuk memastikan pencapaian tujuan yang diinginkan. Adapun Batasan masalah pada penelitian ini adalah sebagai berikut:

1. Model menggunakan arsitektur *hybrid* deep learning berbasis jalur paralel. Convolutional Neural Network (CNN) didedikasikan secara eksklusif untuk mengekstraksi data statis (fitur numerik/kategorikal transaksi), sedangkan Gated Recurrent Unit (GRU) digunakan untuk memproses data temporal (urutan/deret waktu aktivitas), yang output dari keduanya digabungkan melalui *fusion gate*.
2. Dataset yang digunakan adalah IEEE-CIS Fraud Detection [6] yang berisi catatan transaksi e-commerce dari Vesta Corporation.
3. Dataset ini terdiri dari dua tabel, yaitu tabel transaksi dan tabel identitas, dengan total 435 kolom, yang dihubungkan melalui kolom TransactionID. Tidak semua transaksi memiliki informasi identitas yang bersesuaian.

4. Penelitian ini berfokus pada perancangan arsitektur yang ringan guna mengurangi parameter komputasi dan latensi waktu pelatihan yang umumnya menjadi kelemahan pada model hybrid.
5. Target prediksi adalah probabilitas bahwa suatu transaksi online bersifat penipuan, sebagaimana direpresentasikan oleh variabel target biner *isFraud*.
6. Teknik *feature engineering* diterapkan dalam proses pra-pemrosesan data, termasuk penggunaan metode pembuatan *Unique Identifier* (UID) yang mengacu pada pendekatan yang dikembangkan oleh Konstantin Yakovlev dan Chris Deotte pada dataset yang sama.
7. Mekanisme pembentukan penjelasan dalam penelitian ini dibatasi pada dua skenario, yaitu skenario baseline dan skenario hybrid.
8. Evaluasi performa model tidak menjadikan tingkat akurasi sebagai tolak ukur utama keberhasilan, melainkan difokuskan pada metrik yang lebih valid untuk data yang tidak seimbang (*imbalanced data*), meliputi *Area Under Curve* (AUC), Recall (Sensitivity), dan F1-Score.

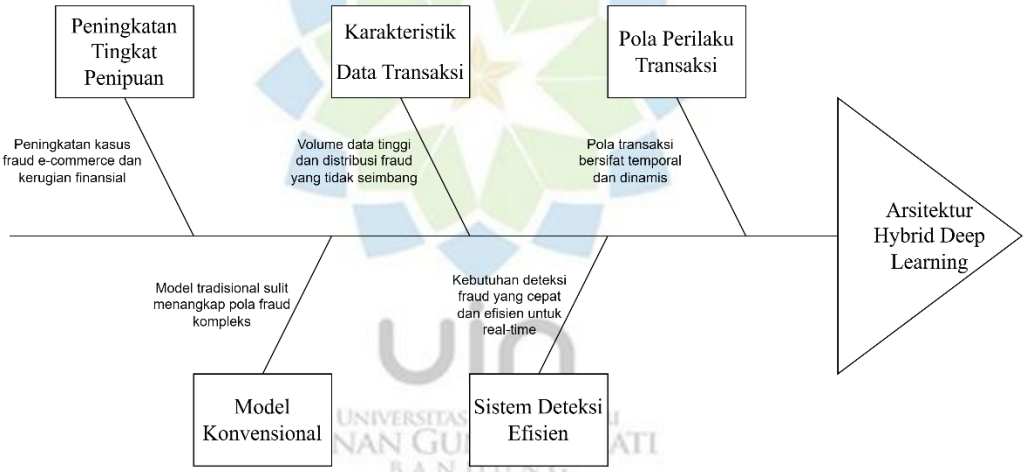
1.4.Tujuan

Berdasarkan rumusan masalah diatas, tujuan dari penelitian ini adalah:

1. Merancang dan mengimplementasikan arsitektur *hybrid* berbasis *deep learning* untuk mendeteksi penipuan pada data transaksi, dengan mengintegrasikan fitur statis dan temporal transaksi.
2. Mengevaluasi kinerja dan efisiensi model *hybrid* dalam mendeteksi penipuan, berdasarkan metrik performa *Receiver Operating Characteristic – Area Under the Curve* (ROC-AUC) dan *Precision Recall – Area Under the Curve* (PR-AUC) serta metrik efisiensi dengan *latency* dan *throughput.*

1.5.Kerangka Pemikiran

Gambar 1.1 menunjukkan kerangka pemikiran yang menjadi acuan dalam penelitian ini. Proses dimulai dari identifikasi masalah, yaitu meningkatnya kasus penipuan pada transaksi e-commerce dengan karakteristik data yang bervolume tinggi, berdistribusi tidak seimbang, serta berpola temporal dan dinamis. Kondisi ini diperparah oleh ketidakmampuan model konvensional dalam menangkap pola penipuan yang kompleks, sekaligus tingginya kebutuhan akan sistem deteksi yang cepat dan efisien untuk keperluan *real-time*. Keseluruhan faktor tersebut secara bersama-sama memotivasi penelitian ini untuk merancang solusi berupa Arsitektur Hybrid Deep Learning sebagai pendekatan yang diharapkan mampu menjawab tantangan tersebut secara komprehensif.



Gambar 1.1 Kerangka Pemikiran