

BAB 1

PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi informasi dalam beberapa tahun terakhir telah mendorong transformasi signifikan pada sistem transaksi keuangan. Aktivitas transaksi yang sebelumnya didominasi oleh penggunaan uang tunai kini semakin berpindah menuju sistem pembayaran digital yang memanfaatkan perangkat *mobile* dan jaringan internet. Perubahan ini terjadi karena sistem pembayaran digital dinilai lebih cepat, praktis, serta efisien dalam mendukung berbagai aktivitas ekonomi masyarakat[1][2].

Salah satu teknologi yang berkembang pesat dalam sistem pembayaran digital adalah penggunaan kode QR (*Quick Response Code*). Teknologi ini memungkinkan proses pembayaran dilakukan dengan cara memindai kode menggunakan kamera pada perangkat *smartphone*. Dibandingkan dengan sistem pembayaran berbasis kartu seperti kartu kredit atau kartu debit yang memerlukan infrastruktur tambahan seperti mesin *Electronic Data Capture* (EDC), pembayaran berbasis QR memiliki keunggulan dari sisi kemudahan implementasi serta biaya infrastruktur yang lebih rendah. Hal ini menjadikan teknologi QR lebih mudah diadopsi oleh berbagai pelaku usaha, terutama pada sektor usaha kecil dan menengah yang mungkin memiliki keterbatasan dalam penyediaan perangkat pembayaran berbasis kartu.

Di Indonesia, implementasi pembayaran berbasis QR semakin berkembang sejak diperkenalkannya standar nasional pembayaran QRIS (*Quick Response Code Indonesian Standard*) oleh Bank Indonesia. Sebelum adanya QRIS, setiap penyedia layanan pembayaran digital memiliki standar kode QR yang berbeda sehingga menyulitkan interoperabilitas antar platform pembayaran. Dengan adanya QRIS, satu kode QR dapat digunakan oleh berbagai aplikasi pembayaran digital sehingga meningkatkan interoperabilitas antar penyedia layanan serta mendorong terciptanya ekosistem pembayaran digital yang lebih terintegrasi dan inklusif[3].

Namun, peningkatan volume transaksi digital juga diikuti dengan meningkatnya potensi risiko keamanan, khususnya terkait aktivitas transaksi yang tidak normal atau mencurigakan yang dapat mengarah pada tindakan *fraud*. Aktivitas tersebut dapat muncul dalam berbagai bentuk, seperti transaksi dengan

nominal tidak wajar, frekuensi transaksi yang tidak biasa, maupun pola transaksi yang berbeda dari perilaku normal pengguna. Dalam sistem pembayaran digital dengan jumlah transaksi yang sangat besar, proses pemantauan transaksi secara manual menjadi tidak efektif untuk mendeteksi aktivitas mencurigakan secara cepat dan akurat[4].

Dalam penelitian ini, istilah anomali merujuk pada transaksi yang memiliki pola menyimpang secara signifikan dibandingkan mayoritas transaksi normal berdasarkan karakteristik data yang dipelajari model [5]. Anomali yang dimaksud berfokus pada aktivitas yang berpotensi terkait *fraud* atau penyalahgunaan transaksi keuangan, seperti nominal transaksi tidak wajar, frekuensi transaksi berlebihan, perubahan saldo yang tidak konsisten, maupun pola transaksi yang berbeda dari perilaku umum pengguna [4].

Pada *dataset PaySim*[6], definisi anomali divalidasi menggunakan label *isFraud = 1* yang merepresentasikan transaksi fraud. Dengan demikian, penelitian ini tidak memfokuskan anomali pada kesalahan sistem teknis atau gangguan perangkat lunak, melainkan pada transaksi mencurigakan yang berpotensi merugikan pihak pengguna maupun penyedia layanan pembayaran digital.

Meskipun demikian, secara konseptual model *anomaly detection* juga dapat mendeteksi perilaku pengguna yang sangat tidak biasa apabila pola tersebut menyimpang dari distribusi normal data. Namun dalam konteks evaluasi penelitian ini, kategori anomali yang dijadikan acuan utama tetap adalah transaksi *fraud* [7].

Untuk mengatasi permasalahan tersebut, berbagai penelitian mulai memanfaatkan pendekatan *machine learning* dalam sistem *fraud detection*[8]. Dengan memanfaatkan data historis transaksi, model *machine learning* mampu mempelajari pola transaksi normal pengguna dan mengidentifikasi transaksi yang memiliki karakteristik berbeda dari pola tersebut melalui pendekatan *anomaly detection*. Beberapa algoritma yang banyak digunakan dalam penelitian deteksi anomali antara lain *Isolation Forest* dan *Autoencoder*. *Isolation Forest* dirancang untuk mengisolasi data yang memiliki karakteristik berbeda dari mayoritas data, sedangkan *Autoencoder* menggunakan pendekatan *neural network* untuk mempelajari pola data normal melalui proses rekonstruksi data[9].

Pemilihan algoritma *Isolation Forest* dan *Autoencoder* dalam penelitian ini didasarkan pada karakteristik keduanya yang efektif untuk menangani permasalahan *anomaly detection* pada data transaksi keuangan yang umumnya bersifat *imbalanced*. Algoritma *Isolation Forest* bekerja dengan cara mengisolasi data yang memiliki karakteristik berbeda dari mayoritas data melalui struktur

pohon acak, sehingga mampu mendeteksi anomali secara efisien pada dataset berskala besar[10].Sementara itu, *Autoencoder* merupakan model *neural network* yang mampu mempelajari representasi pola normal dari data melalui proses rekonstruksi, sehingga transaksi yang memiliki *reconstruction error* tinggi dapat diidentifikasi sebagai anomali. Kombinasi kedua metode tersebut diharapkan dapat memanfaatkan keunggulan masing-masing pendekatan, yaitu kemampuan *Isolation Forest* dalam mendeteksi anomali berbasis struktur data serta kemampuan *Autoencoder* dalam mempelajari pola kompleks pada data transaksi, sehingga dapat meningkatkan performa deteksi transaksi anomali secara lebih akurat dan adaptif.

Meskipun metode *machine learning* mampu meningkatkan kemampuan sistem dalam mendeteksi transaksi anomali, sebagian besar model yang digunakan masih memiliki keterbatasan dalam hal interpretabilitas. Model yang kompleks sering kali bersifat *black-box*, sehingga hasil prediksi yang dihasilkan sulit dipahami oleh pengguna atau analis sistem. Dalam konteks sistem keuangan, kemampuan untuk menjelaskan alasan suatu transaksi dikategorikan sebagai anomali menjadi sangat penting untuk mendukung proses analisis dan pengambilan keputusan[11].

Untuk meningkatkan transparansi model dan kekurangan dari sifat *machine learning* yang bersifat *black-box*, pendekatan *Explainable Artificial Intelligence (XAI)* mulai banyak digunakan dalam sistem deteksi anomali[12]. Metode seperti *SHAP (SHapley Additive exPlanations)* dan *LIME (Local Interpretable Model-agnostic Explanations)* memungkinkan analisis kontribusi setiap fitur terhadap hasil prediksi model. Dengan pendekatan ini, sistem tidak hanya mampu mendeteksi transaksi yang mencurigakan, tetapi juga dapat memberikan penjelasan mengenai faktor-faktor yang mempengaruhi keputusan model[13].

Berdasarkan permasalahan tersebut, penelitian ini mengusulkan pengembangan sistem deteksi transaksi anomali pada pembayaran digital dengan menggunakan pendekatan *Hybrid Machine Learning* yang menggabungkan algoritma *Isolation Forest* dan *Autoencoder*[14]. Pendekatan *hybrid* ini diharapkan mampu memanfaatkan keunggulan masing-masing metode dalam mendeteksi pola anomali pada data transaksi. Selain itu, penelitian ini juga mengintegrasikan metode *Explainable Artificial Intelligence* menggunakan *shap* dan *lime* untuk meningkatkan transparansi dan interpretasi terhadap hasil prediksi model[15].

Dengan pendekatan tersebut, sistem yang dikembangkan diharapkan tidak hanya mampu meningkatkan kemampuan deteksi transaksi anomali secara lebih akurat dan adaptif, tetapi juga mampu memberikan interpretasi yang jelas terhadap keputusan yang dihasilkan oleh model sehingga dapat mendukung penerapan sistem

deteksi *fraud* yang lebih efektif pada sistem pembayaran digital.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan sebelumnya, maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana kinerja model *Hybrid Machine Learning* yang menggabungkan algoritma *Isolation Forest* dan *Autoencoder* dalam mendeteksi transaksi anomali pada sistem pembayaran digital?
2. Bagaimana penerapan metode *hybrid anomaly detection* menggunakan algoritma *Isolation Forest* dan *Autoencoder* dalam mengidentifikasi pola transaksi yang memiliki karakteristik tidak normal?
3. Bagaimana metode *Explainable Artificial Intelligence (XAI)* seperti *SHAP (SHapley Additive exPlanations)* dan *LIME (Local Interpretable Model-agnostic Explanations)* dapat digunakan untuk menjelaskan hasil prediksi model dalam proses deteksi transaksi anomali?

1.3 Batasan Permasalahan

Agar penelitian ini memiliki ruang lingkup yang terfokus dan dapat diselesaikan dengan efisien, maka penelitian ini hanya akan difokuskan pada poin-poin sebagai berikut:

1. Dataset yang digunakan merupakan dataset transaksi digital yang digunakan untuk menganalisis pola transaksi normal dan anomali.
2. Metode deteksi anomali yang digunakan dalam penelitian ini terbatas pada algoritma *Isolation Forest* dan *Autoencoder*.
3. Proses interpretasi hasil prediksi model dilakukan menggunakan metode *Explainable Artificial Intelligence (XAI)* yaitu *SHAP (SHapley Additive exPlanations)* dan *LIME (Local Interpretable Model-agnostic Explanations)*.

1.4 Tujuan Penelitian

Untuk menjawab permasalahan yang telah dirumuskan sebelumnya, maka ditetapkan beberapa tujuan penelitian yang disusun secara sistematis. Tujuan penelitian ini difokuskan pada pengembangan sistem deteksi transaksi anomali pada sistem pembayaran digital dengan memanfaatkan pendekatan *Hybrid Machine Learning* dan *Explainable Artificial Intelligence*. Setiap poin tujuan dibuat agar bisa menjawab langsung rumusan masalah yang telah diajukan:

1. Mengembangkan model *Hybrid Machine Learning* yang menggabungkan algoritma *Isolation Forest* dan *Autoencoder* untuk mendeteksi transaksi anomali pada sistem pembayaran digital.
2. Menganalisis kemampuan metode *hybrid anomaly detection* dalam mengidentifikasi pola transaksi yang memiliki karakteristik tidak normal pada data transaksi keuangan.
3. Menerapkan metode *Explainable Artificial Intelligence (XAI)* menggunakan *SHAP (SHapley Additive exPlanations)* dan *LIME (Local Interpretable Model-agnostic Explanations)* untuk menjelaskan hasil prediksi model deteksi anomali.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan kontribusi baik secara teoritis maupun praktis dalam bidang teknologi informasi, khususnya dalam penerapan metode kecerdasan buatan pada sistem keamanan transaksi digital. Dengan demikian manfaat dari penelitian ini adalah sebagai berikut:

1. Memberikan kontribusi dalam pengembangan ilmu pengetahuan di bidang *machine learning*, khususnya dalam penerapan metode *Isolation Forest* dan *Autoencoder* untuk deteksi transaksi anomali pada sistem pembayaran digital.
2. Menjadi referensi akademis bagi penelitian selanjutnya yang berkaitan dengan pengembangan sistem *fraud detection* berbasis *Hybrid Machine Learning* dan *Explainable Artificial Intelligence (XAI)*.
3. Memberikan pendekatan baru dalam meningkatkan transparansi model *machine learning* melalui pemanfaatan metode *SHAP* dan *LIME* dalam menjelaskan hasil prediksi model.

4. Memberikan kontribusi praktis dalam meningkatkan kemampuan pemantauan transaksi pada sistem pembayaran digital melalui pemanfaatan teknologi *machine learning* dalam mendeteksi aktivitas transaksi yang berpotensi mengarah pada tindakan *fraud*.

1.6 Sistematika Penulisan

Sistematika penulisan laporan adalah sebagai berikut:

a. Bab 1 PENDAHULUAN

Bab ini berisikan latar belakang penelitian, rumusan masalah, batasan permasalahan, serta tujuan dan manfaat dari penelitian yang dilakukan.

b. Bab 2 LANDASAN TEORI

Bab ini berisikan tinjauan teori yang menjelaskan teori-teori yang digunakan sebagai dasar pengetahuan dalam penelitian seperti teori *fraud*, *machine learning*, metode *anomaly detection*, serta algoritma *Isolation Forest* dan *Autoencoder*.

c. Bab 3 METODOLOGI PENELITIAN

Bab ini berisikan alur dan langkah-langkah dari penelitian yang dilakukan, meliputi tahapan penelitian, perancangan sistem, arsitektur sistem, serta penerapan algoritma *machine learning* dalam mendeteksi transaksi anomali.

d. Bab 4 HASIL DAN DISKUSI

Bab ini berisikan hasil implementasi sistem serta analisis yang diperoleh dari penelitian yang dilakukan, termasuk hasil pengujian model *machine learning* dalam mendeteksi transaksi anomali.

e. Bab 5 KESIMPULAN DAN SARAN

Bab ini berisikan kesimpulan yang diperoleh dari hasil penelitian serta saran yang dapat digunakan untuk pengembangan penelitian selanjutnya.