BAB I PENDAHULUAN

A. Latar Belakang Masalah

Era digital saat ini telah mengubah dunia secara dramatis melalui proses digitalisasi. Perubahan ini mencakup hampir semua sektor, termasuk transaksi jual beli, pengiriman surat, transportasi, kesehatan, dan finansial. Saat ini transaksi jual beli tidak lagi membutuhkan pertemuan antara pedagang dan konsumen. Transaksi dapat dilaksanakan secara daring melalui berbagai aplikasi. Surat menyurat pun tidak lagi mengharuskan pengirim untuk datang ke kantor pos dan meminta tukang pos mengantarkannya ke alamat tujuan. Dengan hanya mengetahui alamat surel penerima, pengirim dapat mengirim surat dengan mudah, mencapai tujuan dalam waktu kurang dari satu menit, dengan jangkauan global. Bidang transportasi juga mendapatkan manfaat besar dari era digital ini. Para penumpang yang ingin memesan karcis, saat ini tidak perlu lagi mengantre panjang di depan loket. Calon penumpang dapat dengan mudah memesan tiket secara daring menggunakan aplikasi. Saat ini, konsultasi dengan dokter dapat dilakukan secara daring menggunakan aplikasi. Ini memungkinkan pasien yang hanya memerlukan jawaban atas keluhan mereka untuk menghindari antrean di rumah sakit. Dokter bisa langsung memberikan tanggapan bahkan resep obat jika memang diperlukan atas keluhan tersebut. Sektor finansial juga berhasil memanfaatkan era digital ini dengan efektif. Hampir semua bank telah mengembangkan aplikasi untuk memfasilitasi transaksi nasabahnya. Bahkan perusahaan di bidang keuangan telah merilis aplikasi yang memudahkan masyarakat untuk mengajukan pinjaman.

Digitalisasi memberikan keuntungan berupa kecepatan dan kemudahan bagi penggunanya Namun, kemudahan ini tentu memiliki biaya yang tidak sedikit. Berbagai aspek perlu dipertimbangkan. Salah satunya adalah keamanan pengguna aplikasi tersebut. Awalnya autentikasi pengguna cukup hanya menggunakan password saja. Namun, hal tersebut tidak lagi dianggap aman karena password statis sangat rentan terhadap serangan *brute force*, yaitu upaya menebak password. Salah satu solusi yang saat ini banyak digunakan untuk mengatasi masalah ini adalah One-Time Password (OTP).

OTP adalah teknologi autentikasi yang pertama kali diperkenalkan pada tahun 1980-an oleh perusahaan keamanan seperti RSA Security dan Vasco Data Security. OTP awalnya dikembangkan sebagai solusi untuk masalah yang timbul dari penggunaan password statis atau tetap. OTP dirancang untuk mengatasi kelemahan ini dengan memberikan pengguna password yang berubah setiap kali mereka ingin mengakses sistem atau melakukan transaksi. Dengan demikian, meskipun penyerang

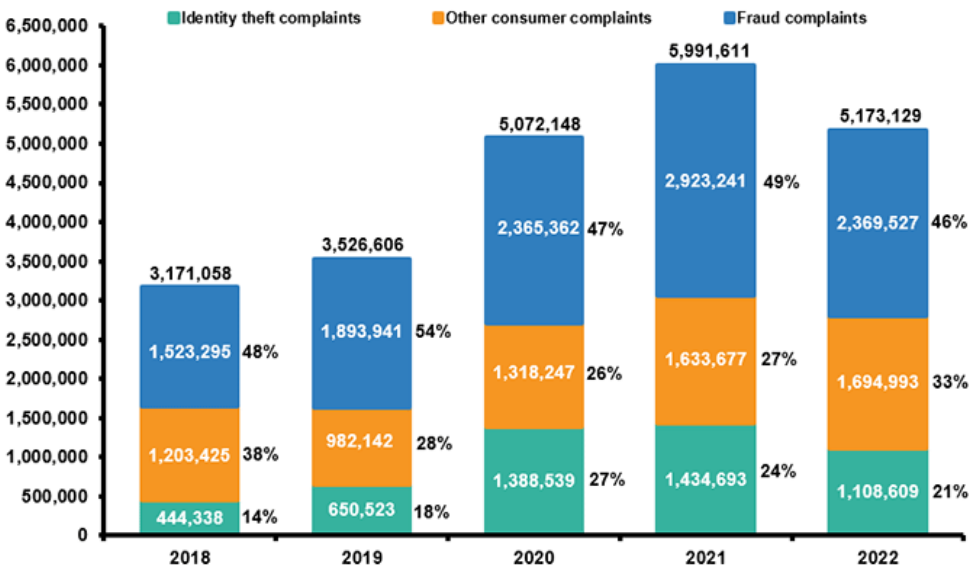
berhasil mendapatkan OTP, mereka tidak dapat menggunakannya lagi karena OTP tersebut hanya berlaku sekali dan akan berubah setelah itu. Tujuan utama pengembangan OTP adalah untuk meningkatkan keamanan sistem dan melindungi data pengguna. Hal ini sangat penting, terutama dalam industri seperti perbankan dan jasa keuangan, di mana perlindungan data dan transaksi pengguna menjadi prioritas utama.

Cara kerja sistem OTP bervariasi, tergantung pada metode yang digunakan. Misalnya, beberapa sistem OTP menggunakan algoritma matematis yang menghasilkan OTP baru setiap kali pengguna melakukan proses autentikasi. Sistem lain mungkin mengirimkan OTP melalui SMS atau surel setiap kali pengguna berupaya mengakses sistem. Selama beberapa dekade terakhir, OTP telah menjadi salah satu metode autentikasi yang sangat umum, terutama dalam konteks transaksi daring dan perbankan seluler.

Penipuan melalui OTP adalah fenomena baru yang muncul seiring dengan peningkatan transaksi digital. Penipuan ini melibatkan pencurian dan penyalahgunaan kode OTP, sebuah kode unik yang seharusnya digunakan untuk autentikasi transaksi atau perubahan informasi penting dalam akun pengguna. Ironisnya, kode ini malah dieksploitasi untuk kegiatan kriminal yang tentunya merugikan banyak pihak.

Skenario kejahatan biasanya melibatkan pelaku yang mencoba untuk mengakses aplikasi menggunakan nomor telepon seluler yang telah dicuri sebelumnya. Saat pelaku ingin mencoba masuk tentunya aplikasi akan meminta kode OTP yang memang dirancang sebagai autentikasi bahwa yang berusaha masuk adalah pemilik asli dari akun tersebut. Pelaku selanjutnya akan menghubungi pemilik asli dari akun dengan berbagai alasan yang dibuat-buat Biasanya, pelaku akan berdalih bahwa pemilik asli akan menerima hadiah dan memerlukan konfirmasi, sehingga meminta pemilik asli untuk mengirimkan OTP yang diterima kepada pelaku. Alasan lain yang biasanya diungkapkan pelaku adalah dengan menyatakan bahwa ada kebijakan baru dari pihak perusahaan yang membuat si pemilik akun asli harus melakukan pembaharuan data yang membutuhkan kode OTP yang diterima pemilik asli untuk konfirmasi kepemilikan.

Kenaikan kasus penipuan OTP menjadi masalah serius dalam sektor keuangan digital. Fenomena ini menciptakan ancaman keamanan bagi pengguna layanan keuangan digital dan perbankan daring. Dampak yang ditimbulkan tidak hanya berupa kerugian finansial, melainkan juga berimbas pada aspek psikologis seperti ketakutan dan penurunan kepercayaan terhadap layanan digital.

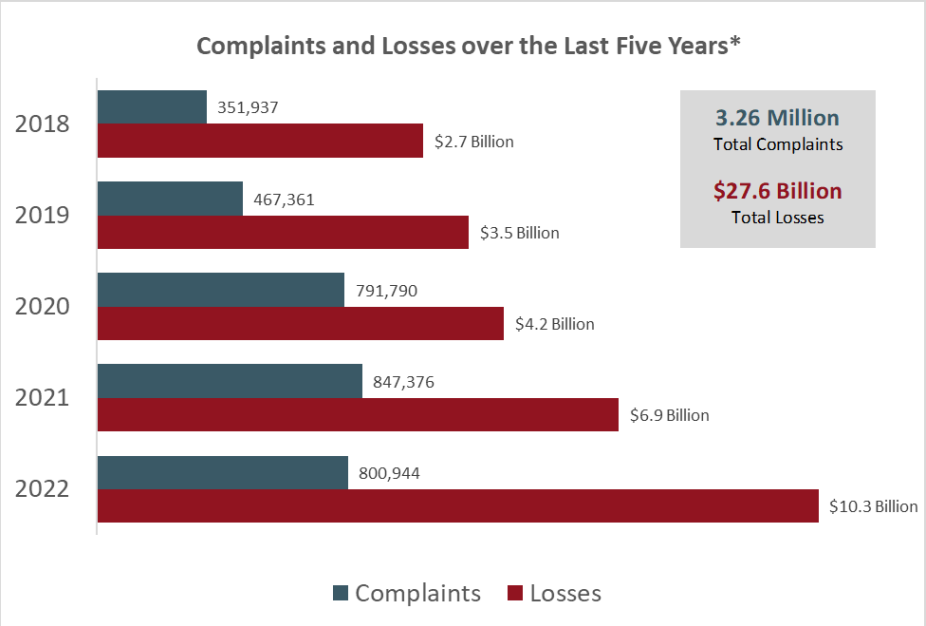


Gambar 1. Laporan pencurian identitas dan penipuan

Sumber: Federal Trade Commission (https://www.iii.org/graph-archive/96074)

Sebagaimana yang ditunjukkan oleh Gambar 1. Data menunjukkan bahwa setiap tahun, keluhan akibat penipuan selalu mendominasi dibandingkan dengan keluhan akibat pencurian identitas. Faktanya, dari tahun 2018 hingga 2022, kasus penipuan selalu memuncak dan memberikan persentase tertinggi di antara kategori pelanggaran lainnya. Pada tahun 2018, penipuan mencapai 48%, pencurian identitas 14%, dan kategori lainnya sebesar 38%. Angka ini meningkat menjadi 54% untuk penipuan pada tahun 2019, dengan pencurian identitas sebesar 18%, dan kategori lain sebesar 28%. Pada tahun 2020, penipuan sedikit berkurang menjadi 47%, namun pencurian identitas naik signifikan menjadi 27%, dan kategori lainnya adalah 26%. Tahun 2021 melihat penipuan meningkat kembali menjadi 49%, dengan pencurian identitas sebesar 24%, dan kategori lain sebesar 27%. Pada tahun 2022, penipuan sedikit berkurang menjadi 46%, dengan pencurian identitas sebesar 21%, dan kategori lain sebesar 33%. Statistik ini menunjukkan bahwa kasus penipuan digital telah menjadi masalah serius.

Sebagaimana yang ditunjukkan oleh Gambar 2. Data menunjukkan peningkatan signifikan dalam jumlah keluhan dan kerugian finansial akibat penipuan OTP selama lima tahun terakhir. Pada tahun 2018, terdapat 351,937 keluhan dengan total kerugian sebesar 2,7 miliar dolar AS. Pada tahun 2022, jumlah keluhan telah naik menjadi 800,944 dengan total kerugian mencapai 10,3 miliar dolar AS. Data ini membuktikan bahwa penipuan OTP telah menjadi masalah yang serius dan memerlukan solusi yang efektif dan segera.



Gambar 2. Laporan keluhan dan kerugian

Sumber: Federal Bureau Of Investigation (https://www.ic3.gov/)

Banyak penelitian telah dilakukan untuk mencari solusi atas masalah penipuan OTP. Misalnya, dengan menambahkan algoritma enkripsi saat melakukan proses autentikasi OTP. Peningkatan metode enkripsi, seperti AES dan Blowfish, dapat mempersulit para pelaku kejahatan dalam melancarkan aksi mereka (D. E. Kurniawan et al., 2021). Walaupun membutuhkan sedikit waktu tambahan, strategi ini dinilai cukup efektif dalam mengurangi masalah penipuan OTP.

Sebuah penelitian lainnya menampilkan algoritma enkripsi gambar berdasarkan urutan kacau dan matriks permutasi, yang memiliki kemampuan untuk menciptakan fitur-fitur semu dan mewujudkan mekanisme kata sandi sekali pakai. Pertama-tama, gambar asli dan matriks yang mengandung informasi kunci inkremental dioperasikan dengan XOR oleh matriks kacau yang dibangun oleh model Logistik. Kemudian, hasilnya ditanamkan dalam matriks yang lebih besar dengan fitur-fitur semu. Akhirnya, matriks permutasi digunakan untuk mengacak posisi piksel gambar untuk mendapatkan gambar yang telah dienkripsi. Hasil simulasi dan analisis keamanan menunjukkan bahwa algoritma enkripsi ini memiliki keunggulan dalam mekanisme kata sandi sekali pakai yang stabil, kapasitas yang kuat untuk menahan berbagai serangan, dan kemampuan untuk menciptakan fitur-fitur semu (Lu et al., 2021).

Sejalan dengan peningkatan kasus penyalahgunaan dan penipuan OTP, kebutuhan akan solusi keamanan yang lebih unggul menjadi sangat mendesak. Metode keamanan tradisional, seperti enkripsi standar dan autentikasi dua faktor, telah terbukti tidak cukup untuk menghadapi penipuan yang semakin canggih ini. Sebuah

Penelitian menunjukkan bahwa nilai-nilai delta moduli RSA-OTP yang ditukar melalui saluran yang tidak aman dapat dikompromikan sepenuhnya, sehingga merusak klasifikasi mereka sebagai elemen OTP (Sarna & Czerwinski, 2022). Oleh karena itu, inovasi dalam sistem keamanan perlu dipertimbangkan, dan salah satu pendekatan yang menunjukkan potensi besar adalah implementasi Pembelajaran Mesin (Machine Learning).

Sebuah penelitian telah dilakukan terkait pemanfaatan Pembelajaran Mesin dalam keamanan digital. Penelitian ini menjelaskan pendekatan berbasis konten, heuristik, dan daftar hitam dalam menghadapi serangan *spoofing* web. Penelitian ini mengembangkan model yang bernama Phish Checker dengan menggunakan Microsoft Visual Studio Express 2013 dan bahasa pemrograman C#. Dengan dataset dari Phish tank dan direktori Yahoo, model ini berhasil mencapai akurasi sebesar 96%.(Kiruthiga & Akila, 2019).

Pembelajaran Mesin merupakan cabang dari Kecerdasan Buatan yang berfokus pada pengembangan dan penerapan algoritma yang memampukan komputer untuk belajar. ML juga memungkinkan komputer untuk membuat keputusan atau prediksi berdasarkan data. Dalam konteks ini, belajar berarti mengidentifikasi dan memahami pola kompleks dalam data tanpa perlu dirancang secara khusus untuk melakukannya. ML dapat dikelompokkan menjadi dua jenis utama: pembelajaran terawasi (*supervised learning*) dan pembelajaran tidak terawasi (*unsupervised learning*).

Supervised learning adalah algoritma yang belajar dari data latih yang telah diberi label. Setiap contoh dalam data latih terdiri dari *input* dan *output* yang diinginkan, yang juga dikenal sebagai label. Algoritma menghasilkan model prediktif berdasarkan pola yang ditemukannya dalam data latih, dan model ini kemudian dapat digunakan untuk memprediksi *output* untuk data baru. Algoritma yang umum digunakan dalam pembelajaran terawasi termasuk regresi linear, regresi logistik, dan random forest.

Unsupervised learning adalah algoritma yang belajar dari data tanpa label. Tujuan utamanya adalah untuk mengeksplorasi struktur dan pola yang mendasari data. Algoritma yang umum dalam pembelajaran tidak terawasi termasuk K-means, klasterisasi hirarkis (*hierarchical clustering*), dan analisis komponen utama (*principal component analysis)*.

Dalam konteks penipuan OTP, Pembelajaran Mesin dapat digunakan untuk membangun model prediktif yang mampu mengenali pola penipuan. Misalnya, dengan *supervised learning*, model dapat dilatih pada sejumlah besar transaksi, di mana setiap transaksi diberi label sebagai penipuan atau bukan penipuan. Selanjutnya model ini dapat digunakan untuk memprediksi apakah transaksi baru merupakan penipuan atau bukan, berdasarkan pola yang telah dipelajarinya dari data latih.

Salah satu algoritma pembelajaran terawasi yang paling populer dan efektif adalah Hutan Acak (Random Forest). Hutan Acak merupakan algoritma Pembelajaran Mesin yang termasuk dalam kategori pembelajaran *ensemble*. Dalam konteks ini berarti metode ini menggabungkan sejumlah model prediktif untuk menghasilkan yang lebih baik daripada masing-masing model secara individu. Dalam kasus random forest, model prediktif yang digunakan adalah pohon keputusan.

Pohon keputusan adalah metode yang efektif untuk klasifikasi dan regresi. Konsepnya cukup sederhana: Proses dimulai dari simpul akar (representasi data), kemudian membaginya menjadi cabang berdasarkan variabel tertentu dari data itu sendiri. Setiap cabang kemudian dibagi lagi, dan proses ini berlanjut sampai mencapai simpul daun, yang merupakan prediksi akhir dari pohon.

Hutan Acak mengambil konsep pohon keputusan dan membawanya ke level yang lebih lanjut. Alih-alih hanya memiliki satu pohon keputusan, Hutan Acak memiliki hutan pohon keputusan. Setiap pohon dalam hutan dibangun sedikit berbeda, menggunakan sub set acak dari data dan/atau sub set acak dari variabel yang tersedia. Ini berarti bahwa setiap pohon memiliki pandangan yang sedikit berbeda terhadap data.

Ketika datang waktu untuk membuat prediksi, Hutan Acak tidak hanya menggunakan satu pohon, tetapi semua pohon dalam hutan. Setiap pohon membuat prediksinya sendiri kemudian prediksi yang paling sering (modus) adalah prediksi akhir dari hutan.

Manfaat utama dari pendekatan ini adalah bahwa Hutan Acak cenderung lebih tahan terhadap *overfitting* dibandingkan dengan pohon keputusan tunggal. *Overfitting* terjadi ketika model terlalu cocok dengan data latihan dan tidak dapat menyesuaikan diri dengan data baru. Karena random forest menggunakan banyak pohon yang dilatih pada sub set data yang berbeda, random forest dapat mencapai keseimbangan yang lebih baik antara kecocokan dengan data latihan dan penyesuaian dengan data baru. Selain itu, Hutan Acak juga memberikan informasi tentang variabel mana yang paling penting dalam membuat prediksi, yang bisa menjadi wawasan yang sangat berharga dalam analisis data.

Sebagai upaya meredam peningkatan kasus penipuan OTP, penelitian ini menawarkan pendekatan berbasis Pembelajaran Mesin, yaitu menggunakan algoritma random forerst. Algoritma ini merupakan teknik pembelajaran mesin yang dapat digunakan untuk tugas klasifikasi dan regresi. Hutan Acak memiliki keunggulan dalam menangani dimensi besar dan mampu menganalisis data dengan banyak variabel, menjadikannya alat yang tepat untuk mengidentifikasi dan mencegah penipuan OTP. Dalam konteks penipuan OTP, setiap pohon keputusan mungkin

menganalisis berbagai aspek dari transaksi, seperti waktu transaksi, lokasi, jumlah transaksi, dan pola transaksi sebelumnya.

Algoritma ini akan belajar dari data transaksi historis dan secara otomatis mengidentifikasi pola yang mencurigakan, yang mungkin menunjukkan penipuan. Dengan kata lain, jika sebuah transaksi memiliki pola yang mirip dengan pola penipuan yang pernah terjadi sebelumnya, sistem akan mengidentifikasinya sebagai transaksi yang berpotensi penipuan dan dapat segera mencegahnya. Algoritma Hutan Acak memberikan pendekatan baru dalam menangani penipuan OTP. Dengan memanfaatkan teknologi ini, kita dapat menciptakan sistem autentikasi yang lebih cerdas dan responsif, yang dapat dengan cepat mendeteksi dan mencegah penipuan. Dengan demikian, kita dapat melangkah lebih dekat ke kondisi ideal di mana pengguna merasa aman dan percaya terhadap platform digital, dan di mana transaksi daring dapat berlangsung tanpa risiko penipuan.

Dalam dunia nyata, sistem autentikasi berbasis OTP telah menjadi alat keamanan yang luas digunakan dalam berbagai platform daring, mulai dari perbankan hingga media sosial. Namun, walaupun OTP dirancang untuk memberikan lapisan keamanan tambahan dalam proses autentikasi, realitas menunjukkan bahwa sistem ini masih rentan terhadap berbagai bentuk penipuan. Penipuan OTP biasanya terjadi ketika penyerang berhasil mendapatkan akses ke OTP yang dikirimkan kepada pengguna, sering kali melalui teknik manipulasi sosial atau *phishing*. Akibatnya, mereka mampu untuk mengakses akun korban dan melakukan berbagai tindakan merugikan. Kondisi ini dibuat semakin parah oleh fakta bahwa banyak pengguna tidak menyadari risiko berbagi OTP mereka dengan orang lain, dan sistem keamanan yang ada sering kali tidak mampu untuk mendeteksi atau mencegah penyalahgunaan ini.

Sebaliknya, kondisi ideal yang diharapkan adalah sistem autentikasi yang sepenuhnya aman dan tidak dapat disalahgunakan oleh penyerang. Dalam konteks ini, sistem ideal adalah yang dapat memberikan pengguna rasa aman bahwa OTP mereka tidak dapat diganggu atau disalahgunakan oleh pihak ketiga. Lebih lanjut, sistem tersebut harus intuitif dan mudah digunakan, sehingga tidak menjadi hambatan bagi pengguna.

Dalam hal ini, teknologi Pembelajaran Mesin seperti Hutan Acak dapat membantu mencapai kondisi ideal tersebut. Algoritma ini mampu untuk belajar dari data historis dan mendeteksi pola penipuan, sehingga dapat memblokir transaksi yang mencurigakan dan mencegah penipuan sebelum terjadi. Kesenjangan antara kondisi nyata dan ideal ini jelas terlihat. Walaupun berbagai upaya telah dilakukan untuk mengatasi penipuan OTP, baik melalui pendidikan pengguna maupun peningkatan

keamanan sistem, fakta bahwa penipuan ini masih terjadi menunjukkan bahwa solusi saat ini belum sepenuhnya efektif.

Berbagai solusi telah diajukan untuk meningkatkan keamanan sistem autentikasi berbasis OTP. Salah satu pendekatan adalah melalui pendidikan pengguna, bertujuan meningkatkan kesadaran pengguna tentang pentingnya menjaga kerahasiaan OTP mereka. Meski memiliki manfaat, pendekatan ini memiliki keterbatasan dalam efektivitas karena bergantung pada pengetahuan dan perilaku individu. Solusi lain melibatkan peningkatan infrastruktur keamanan, seperti penggunaan enkripsi yang lebih kuat atau protokol keamanan yang lebih canggih. Meski berpotensi efektif, solusi ini mungkin memerlukan investasi sumber daya yang signifikan dan mungkin tidak sepenuhnya melawan ancaman penipuan OTP yang menggunakan teknik manipulasi sosial. Solusi lainnya adalah penggunaan teknologi biometri, seperti sidik jari atau pengenalan wajah, sebagai metode autentikasi tambahan. Meski teknologi ini menawarkan tingkat keamanan yang lebih tinggi, namun juga memiliki kekurangan, termasuk masalah keamanan dan potensi penyalahgunaan data.

Di antara berbagai solusi yang telah disebutkan, penggunaan Pembelajaran Mesin, khususnya algoritma Hutan Acak, menonjol sebagai pendekatan yang paling menjanjikan. Algoritma Hutan Acak adalah metode Pembelajaran Mesin yang menggunakan sejumlah pohon keputusan untuk membuat prediksi atau klasifikasi berdasarkan data masukan. Dalam konteks keamanan OTP, algoritma ini dapat belajar dari data transaksi sebelumnya untuk mendeteksi pola-pola yang mencurigakan dan mencegah penipuan sebelum terjadi. Kelebihan utama pendekatan ini adalah bahwa ia tidak bergantung pada perilaku pengguna atau infrastruktur keamanan yang ada, melainkan pada analisis data yang objektif dan sistematis.

Ada juga beberapa kekurangan yang perlu dipertimbangkan. Misalnya, implementasi sistem Pembelajaran Mesin dapat memerlukan investasi waktu dan sumber daya yang signifikan. Selain itu, kualitas prediksi atau klasifikasi yang dibuat oleh model tergantung pada kualitas data yang digunakan untuk melatih model tersebut. Meski ada kekurangan, algoritma Hutan Acak menawarkan pendekatan yang paling komprehensif dan efektif untuk mengatasi masalah penipuan OTP. Dengan kemampuannya untuk belajar dari data dan mendeteksi penipuan sebelum terjadi, teknologi ini memberikan harapan untuk mencapai kondisi keamanan OTP yang ideal. Oleh karena itu, mempelajari dan menerapkan algoritma ini lebih lanjut dalam konteks keamanan OTP adalah langkah yang penting dan diperlukan.

Dalam menerapkan algoritma Hutan Acak sebagai solusi penipuan OTP, berbagai tantangan dan hambatan mungkin akan dihadapi. Pertama, tantangan utama adalah membangun dan melatih model Pembelajaran Mesin itu sendiri. Ini memerlukan

pengetahuan dan keterampilan yang cukup dalam bidang Pembelajaran Mesin, serta akses ke data pelatihan yang relevan dan komprehensif. Selain itu, untuk menghasilkan prediksi yang akurat dan efektif, model tersebut perlu dilatih secara berkala dengan data terbaru.

Selanjutnya ada tantangan teknis dan infrastruktur. Meski teknologi komputasi awan terdistribusi telah mempermudah skala dan efisiensi pengolahan data, namun implementasi algoritma Pembelajaran Mesin pada skala yang besar masih memerlukan investasi infrastruktur yang signifikan. Selain itu, menjaga keamanan dan privasi data selama proses ini juga merupakan tantangan yang harus dihadapi.

Tantangan lain yang mungkin muncul datang dari sisi hukum dan regulasi. Di banyak yurisdiksi, penggunaan data untuk tujuan seperti ini diatur oleh undang-undang privasi dan perlindungan data. Oleh karena itu, pihak yang berwenang harus memastikan bahwa semua penggunaan data pelanggan mematuhi hukum dan peraturan yang berlaku.

Di sisi lain, ada juga berbagai faktor yang dapat mendukung keberhasilan implementasi solusi ini. Pertama, perkembangan teknologi dan infrastruktur komputasi atau yang biasa kita kenal dengan komputasi awan terdistribusi telah mempermudah implementasi algoritma Pembelajaran Mesin pada skala yang besar. Selain itu, pengetahuan dan keterampilan dalam bidang ini semakin tersebar luas, berkat pendidikan dan pelatihan yang tersedia secara luas. Faktor pendukung lainnya adalah keinginan yang kuat dari berbagai pihak untuk meningkatkan keamanan OTP dan mengurangi penipuan. Ini menciptakan motivasi dan dukungan untuk mencari dan menerapkan solusi baru dan lebih baik. Ada juga faktor kesadaran yang semakin besar tentang pentingnya perlindungan data dan privasi, serta pengetahuan tentang bagaimana teknologi seperti Pembelajaran Mesin dapat membantu dalam hal ini. Oleh karena itu, ada peluang yang baik bahwa solusi seperti ini akan diterima dan didukung oleh masyarakat luas. Mengingat tantangan dan pendukung ini, sangat penting untuk merencanakan dan mengelola implementasi algoritma Hutan Acak dengan hati-hati. Meski ada hambatan, namun dengan perencanaan, pelatihan, dan dukungan yang tepat, ada peluang besar untuk mengatasi tantangan ini dan mencapai tujuan keamanan OTP yang lebih baik.

Solusi yang ditawarkan dalam penelitian ini, yaitu implementasi algoritma Hutan Acak, dapat membantu mengatasi masalah penipuan OTP dengan memprediksi dan mencegah aktivitas mencurigakan. Algoritma ini dapat belajar dari pola dan kecenderungan dalam data historis dan menggunakan pengetahuan ini untuk mengidentifikasi dan mencegah penipuan OTP. Dengan demikian, penelitian ini dapat

membantu memperkuat sistem autentikasi dan meningkatkan kepercayaan konsumen terhadap transaksi daring.

Penelitian ini juga bisa dijadikan acuan oleh pihak lain di masa mendatang untuk memperbaiki dan mengembangkan sistem keamanan mereka. Misalnya, penyedia layanan digital dapat menggunakan hasil penelitian ini sebagai landasan untuk memperbaiki sistem autentikasi mereka. Peneliti di bidang keamanan siber dan Pembelajaran Mesin juga dapat memanfaatkan temuan ini untuk memperluas pengetahuan mereka dan mengembangkan solusi keamanan yang lebih efektif. Dalam jangka panjang, penelitian ini dapat berkontribusi pada perkembangan teknologi keamanan digital dan mendorong inovasi dalam bidang ini. Dengan demikian, penelitian ini tidak hanya penting untuk mengatasi masalah penipuan OTP saat ini, tetapi juga berpotensi membantu mendorong perkembangan dan peningkatan di bidang keamanan digital di masa mendatang. Berdasarkan pertimbangan tersebut, penelitian ini diberi judul “Implementasi Algoritma Random Forest Untuk Optimasi Keamanan Autentikasi One-Time Password (OTP)

B. Permasalahan

Salah satu cara untuk menjaga keamanan informasi saat melakukan transaksi atau mengakses suatu aplikasi adalah dengan menggunakan One-Time Password (OTP), yaitu sebuah kata sandi yang hanya dapat digunakan sekali dan dalam waktu yang terbatas. Namun, cara ini tidak sepenuhnya aman dari ancaman kejahatan siber, seperti penipuan daring (phishing) dan serangan lain yang bisa menyebabkan kehilangan data atau akses ilegal. Oleh karena itu, diperlukan upaya untuk meningkatkan sistem keamanan OTP.

Tabel 1. Daftar riwayat transaksi OTP

no	1	2	3	4
otp_id	3994c011- 73a	6eada426-ac3	c78371c3-22a	18b60746-cf2
Merchant_id	1	1	1	1
pic_id	085811751000	085811751000	085811751000	085811751000
purpose	LOGIN	LOGIN	LOGIN	TRANSACTION
latitude	-6.6502314	-6.6502314	28.61318	-6.6494934
longitude	106.7560309	106.7560309	77.209153	106.7557339
device_name	SM-A235F	SM-A235F	Xiaomi Redmi Note 10	SM-A235F
os_version	14	14	13	14
manufacturer	samsung	samsung	Xiaomi	samsung

cpu_info	Qualcomm Technologies, Inc KHAJE	Qualcomm Technologies, Inc KHAJE	Snapdragon 865	Qualcomm Technologies, Inc KHAJE
platform	ANDROID	ANDROID	ANDROID	ANDROID
otp	3004	7637	8045	7847
ip	192.168.1.34	192.168.1.34	203.123.123.123	10.5.248.250
is_active	False	False	False	False
created_at	2023-09-23 00:51:58	2023-09-23 00:54:57	2023-09-17 02:17:48	2023-09-15 01:50:38
expired_at	2023-09-23 00:54:58	2023-09-23 00:57:57	2023-09-17 02:20:48	2023-09-15 01:53:38
updated_at	2023-09-23 00:52:37	2023-09-23 00:55:44	2023-09-17 02:17:58	2023-09-15 01:50:53

Sumber: PT Fazpass Integrasi Indonesia

Berdasarkan Tabel 1, tampak bahwa catatan transaksi permintaan OTP hanya mencerminkan riwayat berdasarkan klien dan perusahaannya. Transaksi OTP pada entri nomor 3 menunjukkan perilaku yang signifikan berbeda dibandingkan dengan riwayat transaksi OTP lainnya. Transaksi pada entri nomor 3 tampaknya menggunakan perangkat yang berbeda, IP yang tidak sama, serta lokasi permintaan yang sangat berbeda dari transaksi lainnya. Idealnya, permintaan ini tidak seharusnya dilayani karena dapat dianggap sebagai anomali. Namun, karena tidak adanya sistem yang mampu mendeteksi permintaan transaksi semacam ini, ada kebutuhan untuk optimasi berorientasi preventif agar tidak semua permintaan OTP dilayani tanpa pertimbangan.

1. Identifikasi Masalah

Berdasarkan pemaparan permasalahan di atas, maka dapat diidentifikasi masalah penelitian & pengembangan ini, adalah:

a. Belum optimal untuk mengklasifikasi transaksi penipuan autentikasi OTP.
b. Belum efektif mendeteksi dan pencegahan penipuan autentikasi OTP.

2. Rumusan Masalah

Berdasarkan identifikasi masalah di atas, maka dapat ditetapkan pokok masalah (problem statement) dari penelitian & pengembangan ini adalah ketidak optimalan sistem dalam mengklasifikasi dan mendeteksi transaksi penipuan autentikasi OTP, serta kebutuhan untuk meningkatkan pencegahan dan keamanan autentikasi.

Pertanyaan penelitian (research question) yang dapat diajukan, adalah:

a. Bagaimana penerapan algoritma Random Forest dapat memperbaiki akurasi deteksi transaksi penipuan pada autentikasi OTP.
b. Bagaimana proses optimalisasi pengamanan autentikasi dilakukan untuk mencegah penipuan.

C. Maksud dan Tujuan Penelitian

1. Maksud Penelitian

Maksud dari penelitian ini adalah melakukan optimasi autentikasi OTP dalam transaksi digital. Untuk mencapai tujuan tersebut, penelitian ini dirancang untuk mengimplementasikan sistem deteksi dan pencegahan penipuan OTP yang efisien dan efektif. Tugas utama yang perlu dilakukan adalah pembangunan model berbasis algoritma Random Forest, yang memiliki kemampuan mendeteksi dan mencegah penipuan OTP secara real-time.

2. Tujuan Penelitian

Penelitian ini bertujuan untuk meningkatkan pemahaman mengenai efektivitas algoritma Random Forest dalam mendeteksi dan mencegah penipuan OTP, dan untuk meningkatkan kepercayaan pengguna dalam melakukan transaksi digital. Secara spesifik, tujuan dari penelitian ini adalah:

a. Mengevaluasi efektivitas dan efisiensi algoritma Random Forest dalam mendeteksi dan mencegah penipuan OTP.
b. Mengidentifikasi kelemahan dan kekuatan model yang digunakan dalam mendeteksi dan mencegah penipuan OTP secara real-time.
c. Memberikan rekomendasi untuk peningkatan model deteksi dan pencegahan penipuan OTP berdasarkan hasil evaluasi

D. Spesifikasi Produk yang Diharapkan

Produk yang diperoleh dari penelitian dan pengembangan ini berbentuk API (*Application Programming Interface),* yang dirancang untuk mendeteksi dan mencegah penipuan OTP dalam lingkungan transaksi digital secara real-time. API ini berfungsi sebagai alat penting untuk memastikan integritas dan keamanan transaksi.

Berikut adalah spesifikasi rinci dari API tersebut:

1. Model Prediktif: API ini dilengkapi dengan model prediktif yang dikembangkan dengan menggunakan algoritma Random Forest. Model ini memanfaatkan fitur-fitur yang relevan dalam deteksi penipuan OTP, seperti pola penggunaan, lokasi, dan waktu transaksi.
2. Deteksi Real-time: API ini memiliki kemampuan untuk mendeteksi penipuan OTP secara real-time, sehingga penipuan dapat segera diidentifikasi dan dicegah.
3. Interoperabilitas: API ini dirancang dengan fokus pada kemudahan integrasi dengan sistem lain, memungkinkannya untuk diterapkan pada berbagai platform transaksi digital untuk meningkatkan keamanannya.
4. Pembaruan Model: API ini termasuk fitur pembaruan model yang memungkinkan model untuk belajar dan diperbarui berkelanjutan berdasarkan data terbaru. Hal

ini memastikan bahwa model tetap relevan dan efektif dalam mengidentifikasi penipuan OTP.

5. Ramah Pengguna: Meski operasionalnya kompleks, API ini dirancang untuk mudah digunakan. Semua fitur dapat diakses dengan mudah, dan dokumentasi yang jelas disertakan untuk membantu pengguna.

Dengan spesifikasi tersebut, produk yang dihasilkan ini diharapkan menjadi solusi yang efektif dalam penanganan penyalahgunaan kode OTP dalam transaksi digital.

E. Signifikansi Penelitian

Signifikansi penelitian ini terletak pada urgensi untuk memperbaiki kondisi keamanan transaksi digital yang saat ini rentan terhadap penyalahgunaan OTP. Dalam konteks yang lebih luas, penipuan OTP tidak hanya merugikan pengguna secara finansial, tetapi juga merusak kepercayaan mereka terhadap transaksi digital. Akibatnya, perkembangan digital ekonomi dapat terhambat dan ini menjadi permasalahan serius mengingat pentingnya peran digital ekonomi dalam era digital saat ini.

Selain itu, penelitian ini juga memiliki signifikansi dalam pengembangan teknologi keamanan digital. Dengan mengembangkan sistem deteksi dan pencegahan penipuan OTP yang efektif, penelitian ini dapat membantu mendorong inovasi dan perkembangan di bidang keamanan digital. Ini berarti bahwa hasil dari penelitian ini tidak hanya dapat membantu dalam menangani masalah penipuan OTP, tetapi juga berpotensi memberikan kontribusi pada peningkatan keamanan digital secara umum.

Akhirnya, penelitian ini juga penting dalam konteks hukum dan etika. Dengan meningkatkan keamanan transaksi digital, penelitian ini dapat membantu dalam memastikan bahwa transaksi digital dilakukan dengan cara yang adil dan etis, dengan memastikan bahwa hak dan privasi pengguna dilindungi. Oleh karena itu, penelitian ini memiliki signifikansi yang besar tidak hanya dalam konteks teknologi, namun juga dalam konteks sosial dan etika.

F. Asumsi dan Keterbatasan

1. Asumsi Pengembangan

a. Algoritma Random Forest Efektif: Penelitian ini mengasumsikan bahwa algoritma Random Forest adalah metode yang efektif untuk mendeteksi dan mencegah penipuan OTP. Asumsi ini didasarkan pada penelitian-penelitian sebelumnya yang telah membuktikan efektivitas algoritma ini dalam berbagai aplikasi *machine learning*.

b. Ketersediaan Data: Penelitian ini mengasumsikan bahwa data transaksi yang relevan dan mencukupi tersedia untuk melatih dan menguji model. Ini penting

karena kualitas dan kuantitas data yang digunakan akan sangat mempengaruhi kualitas prediksi model.

2. Keterbatasan Pengembangan

a. Lingkup Penggunaan: Meskipun sistem yang dikembangkan diharapkan dapat mendeteksi dan mencegah penipuan OTP dengan efektif, namun penggunaannya paling efektif dalam konteks transaksi digital.
b. Dependensi pada Data: Efektivitas sistem sangat bergantung pada kualitas data yang digunakan. Jika data yang digunakan tidak akurat, tidak lengkap, atau bias, hal ini dapat mempengaruhi kualitas prediksi model.
c. Perubahan Pola Penipuan: Penjahat siber terus mengembangkan metode baru untuk melakukan penipuan. Oleh karena itu, meskipun sistem ini dirancang untuk dapat belajar dan beradaptasi dengan perubahan, namun masih ada kemungkinan sistem ini gagal mendeteksi beberapa metode penipuan yang sangat baru atau canggih.

G. Definisi Istilah dan Definisi Operasional

Berikut adalah beberapa definisi istilah dan definisi operasional yang mungkin relevan:

1. One-Time Password (OTP): Kode autentikasi yang unik dan hanya berlaku untuk satu kali transaksi atau sesi login. OTP digunakan untuk memastikan bahwa pengguna yang berusaha masuk atau melakukan transaksi adalah pengguna yang sah.
2. Penipuan OTP: Aktivitas ilegal di mana kode OTP dicuri atau dipalsukan oleh penjahat siber untuk melakukan transaksi atau akses yang tidak sah.
3. API (Application Programming Interface): Sebuah antarmuka yang memungkinkan dua aplikasi untuk berkomunikasi satu sama lain. Dalam konteks penelitian ini, API mengacu pada sistem deteksi dan pencegahan penipuan OTP yang dapat terintegrasi dengan platform transaksi digital lainnya.
4. Real-time Detection: Kemampuan sistem untuk mendeteksi dan mencegah penipuan OTP saat itu juga atau dalam waktu nyata. Dalam penelitian ini, hal ini berarti bahwa sistem mampu mengidentifikasi dan mencegah penipuan segera setelah kode OTP dimasukkan atau transaksi dilakukan.
5. Interoperabilitas: Kemampuan sebuah sistem untuk bekerja atau beroperasi dengan sistem lain. Dalam konteks penelitian ini, ini berarti bahwa sistem deteksi dan pencegahan penipuan OTP yang dikembangkan dapat terintegrasi dan bekerja dengan berbagai platform transaksi digital.