BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Smartphone merupakan suatu inovasi baru dalam proses komunikasi. *Smartphone* adalah semacam komputer mini yang juga berfungsi sebagai alat komunikasi, memberikan banyak manfaat bagi penggunanya. Keamanan adalah hal yang sangat penting dalam mengoperasikan sistem ini, terutama ketika harus menjaga kerahasiaan informasi, terutama yang bersifat sensitif dan hanya boleh diakses oleh pihak yang berwenang. Sistem ini harus memiliki tingkat keamanan yang tinggi untuk memastikan bahwa pengguna merasa aman dan nyaman, terhindar dari gangguan dan serangan dari luar seperti spam atau virus.[1]

Pada era globalisasi yang sedang berlangsung, perkembangan teknologi berkembang pesat. *Smartphone* menggunakan berbagai sistem operasi seperti *IOS, Windows Phone*, dan Android. Android adalah sistem operasi yang paling banyak digunakan di seluruh dunia saat ini, dengan banyaknya aplikasi yang bertujuan untuk mempermudah kehidupan sehari-hari. Banyak di antara aplikasi yang tersedia untuk *Smartphone* Android, terdapat beberapa yang berpotensi berbahaya dan dapat membahayakan pengguna dan perangkat.[2]

Mobile Security Framework (MobSF) adalah suatu kerangka kerja yang digunakan dalam pengujian penetrasi pada aplikasi seluler, termasuk platform Android, iOS, dan Windows. *MobSF* dapat melakukan analisis statis, dinamis, serta deteksi malware secara otomatis. *MobSF* menggunakan alat analisis statis dan dinamis yang mengandalkan DroidMon-Dalvik Monitoring Framework dan Xposed Module Repository. Xposed adalah kerangka kerja yang memungkinkan modifikasi perilaku sistem dan aplikasi tanpa harus menyentuh file APK asli. Hal ini memungkinkan modul-modul yang dikembangkan untuk berfungsi pada berbagai versi perangkat dan bahkan ROM tanpa perubahan yang signifikan

pada kode asli. *MobSF* menjadi alat yang sangat berguna dalam mengidentifikasi potensi kerentanan keamanan dalam aplikasi seluler dan membantu dalam meningkatkan keamanan aplikasi tersebut sepanjang siklus pengembangan.[3]

Indonesia mengalami peningkatan kejahatan dunia maya, seperti kebocoran data yang terus berlangsung. Salah satu kasus yang mencolok adalah pencurian data pada aplikasi mobile *E-commerce* di Indonesia. Hasil dari penelitian sebelumnya mengungkap bahwa sekitar 91 juta titik data pengguna aplikasi Tokopedia diperdagangkan secara ilegal di situs Dark Web. Data pribadi pengguna, seperti email, nama, alamat, tanggal lahir, dan nomor telepon, mungkin telah terekspos. Pelaku menjual data ini dengan harga *$5.000* atau sekitar Rp74 juta. Kejadian ini terjadi karena masalah kecerobohan dan kerentanan sistem keamanan teknologi online, yang berdampak buruk bagi pengguna dan pemilik platform. Pada umumnya, penyedia aplikasi mobile *E-commerce* meminta izin pengguna untuk mengakses data pribadi mereka, seperti email, alamat, dan nomor telepon. Informasi pribadi seperti email, alamat, dan nomor telepon adalah hal yang unik dan dapat disalahgunakan. Berdasarkan penelitian sebelumnya, kasus kebocoran akun di Indonesia mengalami peningkatan lebih dari 100% dari tahun 2021 ke tahun 2022, menjadikan Indonesia sebagai salah satu negara dengan peningkatan terbesar dalam kasus kebocoran akun selama periode tersebut. Ancaman terhadap keamanan siber tidak terlepas dari masalah kecerobohan dan kerentanan sistem keamanan teknologi online yang berdampak negatif bagi pengguna aplikasi dan pemilik platform. Mengingat peningkatan pengguna perdagangan elektronik di Indonesia yang diperkirakan mencapai 189,6 juta pada tahun 2024, penting bagi semua pihak yang terlibat dalam transaksi online untuk mempertimbangkan ancaman terhadap keamanan informasi dan menggali pengetahuan yang relevan dan up-to-date untuk mengurangi risiko. Pengembangan sistem pengujian keamanan bertujuan untuk mencari kode yang akan dianalisis dengan menerapkan teknik Analisis Statis *OWASP Mobile Application Security Testing Guide (MASTG)*. Hasil dari sistem ini dapat digunakan untuk evaluasi lebih lanjut berdasarkan pedoman *OWASP MASTG*. Pada konteks

pengujian keamanan seluler Android, ada serangkaian fase yang dianjurkan oleh *OWAS*P, yang biasanya digunakan oleh penguji penetrasi, termasuk persiapan, pengumpulan data yang cerdas, pemetaan aplikasi, eksploitasi, dan pelaporan.[4]

Pentingnya keamanan dalam *(E-Commerce)* dan peran kriptografi dalam melindungi data pelanggan dan informasi rahasia. Benar bahwa keamanan sangat penting dalam transaksi online, terutama mengingat risiko pencurian data dan kebocoran informasi yang bisa merugikan pelanggan dan penyedia layanan. Penggunaan kriptografi adalah langkah yang bijak untuk melindungi data transaksi dan informasi pelanggan. Penting untuk memahami bahwa dalam ekosistem *E-commerce*, ada banyak komponen yang terlibat, seperti konsumen, penjual, produk, sistem front-end dan back-end, infrastruktur, mitra bisnis, dan layanan pendukung. Semua komponen ini harus berjalan dengan baik dan aman untuk memastikan keberhasilan sistem *E-commerce*. Keamanan harus mencakup distribusi barang yang aman, sistem pembayaran yang terlindungi, dan perlindungan data dan informasi yang kuat. Sehingga memberikan keyakinan kepada konsumen dan memastikan bahwa transaksi *E-commerce* berjalan dengan lancar dan aman bagi semua pihak yang terlibat. Penerapan aturan dan kebijakan yang ketat dalam sistem *E-commerce* juga menjadi faktor penting dalam menjaga keamanan dan integritas transaksi online.[5]

Emulator adalah pendekatan yang populer, ekonomis, mudah diimplementasikan, dan fleksibel dalam menjalankan aplikasi, sehingga menjadi pilihan dalam banyak penelitian. Hasil dari pengujian emulator ini sering dianggap mewakili perilaku aplikasi Android pada semua perangkat, baik asli maupun emulator. Penelitian tentang deteksi malware Android tidak memiliki fokus tunggal dalam hal jenis perangkat yang digunakan. Terdapat juga variasi dalam penggunaan platform emulator, mulai dari emulator resmi Android hingga *sandbox* pendeteksi *malware* Android yang disesuaikan. Tidak ada interaksi yang dilakukan dengan aplikasi selain dari proses awal, yaitu *booting* menggunakan *monkey tool* untuk Android. Pada

kedua perangkat, konfigurasi dasar Android 8.0 yang sama telah diatur, termasuk menonaktifkan tindakan keamanan, mengaktifkan koneksi *Wi-Fi,* menginstal *Google Play*, dan menghilangkan kartu SIM.[6]

Penggunaan teknologi *Smartphone* berbasis Android sangat umum karena menyediakan berbagai layanan, fitur, dan aplikasi yang mendukung produktivitas. Salah satu jenis aplikasi yang sering digunakan oleh pengguna Android adalah aplikasi *E-commerce* atau belanja online. Aplikasi *E-commerce* berbasis Android memungkinkan pengguna untuk berbelanja dan melakukan transaksi online melalui *Smartphone* mereka dengan mudah dan cepat. Popularitas aplikasi *E-commerce* di Indonesia, yang sering diunduh dari *Play Store*, memiliki potensi risiko keamanan. Beberapa aplikasi *E-commerce* dapat meminta izin akses yang luas ke berbagai fitur ponsel, seperti kontak, penyimpanan file, kamera, dan lokasi. Ini dapat membuka peluang bagi malware untuk mengambil data pengguna. Selain itu, perangkat *Smartphone* saat ini menjadi sumber penting bukti digital dalam investigasi, terutama terkait dengan penggunaan aplikasi dan media sosial. Mobile forensik menjadi penting dalam mengidentifikasi ancaman malware dengan menganalisis izin akses yang diminta oleh aplikasi. Pengguna seringkali tidak memahami sepenuhnya risiko dan tujuan dari izin akses yang diminta oleh aplikasi sebelum atau setelah menginstalnya, maka dari itu forensik mobile merupakan pendekatan yang sangat diperlukan.[7]

Perilaku konsumen yang cenderung menggunakan aplikasi mobile dalam berbelanja online membuat pelaku *E-commerce* harus fokus pada optimalisasi pengalaman pengguna (*UI* dan *UX*) pada aplikasi mereka. Pemberian promo eksklusif bagi pengguna aplikasi juga dapat menjadi strategi yang efektif untuk meningkatkan kepercayaan dan loyalitas pelanggan. Selain potensi dan manfaatnya, *E-commerce* juga memiliki tantangan keamanan yang signifikan. Celah-celah keamanan dalam aplikasi *E-commerce* dapat menjadi target bagi penyerang untuk mencuri informasi penting yang disimpan dalam *Smartphone* pengguna. Informasi ini bisa

sangat berharga dan berkisar dari catatan, komunikasi lisan, data elektronik, hingga konten audio visual. *E-commerce* telah berkembang pesat di Indonesia, belum banyak penelitian yang memfokuskan pada analisis celah-celah keamanan dalam aplikasi *E-commerce* yang banyak digunakan di negara ini. Analisis keamanan aplikasi *E-commerce* secara menyeluruh penting untuk dilakukan.[8]

E-commerce telah menjadi salah satu cara yang populer untuk berbelanja dan menjual produk atau jasa. Banyak platform *E-commerce* yang tersedia, seperti Shopee, Lazada, Blibli, Tokopedia, dan banyak lainnya, yang menawarkan berbagai kemudahan bagi konsumen. Beberapa tantangan atau masalah yang dapat ditemui ketika berbelanja online, seperti produk yang tidak sesuai dengan deskripsi, kualitas yang kurang memuaskan, masalah keamanan, pelayanan yang kurang memuaskan, dan juga pembatasan penggunaan *voucher* atau promo tertentu. Sehingga hal ini membantu konsumen dalam memilih *E-commerce* yang terbaik untuk kebutuhan mereka atau peringkat e-commerce dapat menjadi alat yang berguna. *E-commerce*, sebagai bentuk perdagangan elektronik, memang memiliki potensi yang besar dengan kemajuan teknologi internet dan penggunaan perangkat mobile yang semakin meluas. Penting juga bagi konsumen untuk tetap waspada dan memilih *E-commerce* dengan bijak untuk meminimalkan risiko yang mungkin timbul selama proses berbelanja online. Selain itu, *E-commerce* juga perlu terus berinovasi dan meningkatkan pelayanannya untuk memenuhi harapan konsumen.[9]

Sebagai perusahaan startup yang bergerak dalam industri kedai kopi, fore coffe memiliki model bisnis yang unik dengan fokus utama pada memenuhi kebutuhan pencinta kopi di Indonesia. Aplikasi mobile khusus yang dapat diunduh oleh pengguna perangkat iOS melalui App Store dan Google PlayStore juga telah dikembangkan oleh fore coffe. Kepuasan pengguna terhadap aplikasi dapat diukur dengan mengadopsi pendekatan analisis sentimen.

Analisis sentimen adalah pendekatan yang populer untuk memahami pandangan dan perasaan pengguna terhadap suatu produk atau layanan.[10]

Perkembangan bisnis online telah memberikan banyak manfaat dan kemudahan bagi konsumen, termasuk dalam hal pembelian barang dan jasa serta pembayaran. Uber dan Grab adalah pesaing utama Gojek dalam hal layanan transportasi dan pengiriman makanan. Persaingan ini memungkinkan konsumen untuk memiliki lebih banyak pilihan, tetapi juga mendorong penyedia layanan untuk meningkatkan kualitas dan menawarkan insentif seperti *voucher* promo untuk menarik lebih banyak pelanggan. Pada konteks penggunaan *voucher* promo, penting untuk mempertimbangkan aspek hukum persaingan usaha. Pada Undang-Undang No 5 tahun 1999 tentang Persaingan Usaha dan Anti Monopoli yang mengatur persaingan usaha yang sehat. Pasal 20 dari undang-undang tersebut melarang pelaku usaha menjual dengan kerugian atau dengan harga yang sangat rendah untuk menghilangkan pesaingnya dari pasar, yang dapat dianggap sebagai perilaku monopoli atau ketidakadilan dalam persaingan usaha. Pemberian *voucher* promo oleh Gojek, jika digunakan untuk menarik lebih banyak pelanggan dan meningkatkan persaingan dengan cara yang sah, mungkin tidak melanggar undang-undang tersebut. Sehingga penting juga bagi pelaku usaha untuk memastikan bahwa penggunaan *voucher* promo tidak bertujuan untuk menghilangkan pesaing atau menciptakan praktik persaingan usaha yang tidak sehat. Pada akhirnya, penting untuk memahami bahwa penerapan undang-undang persaingan usaha adalah tanggung jawab otoritas yang berwenang dan bisa berbeda-beda di berbagai negara. Langkah yang bijak dalam menjawab pertanyaan atau keraguan tentang legalitas suatu strategi pemasaran atau penggunaan *voucher* promo dapat dikonsultasikan dengan ahli hukum yang berpengalaman dalam hukum persaingan usaha.[11]

Perkembangan teknologi yang pesat telah mengubah banyak aspek kehidupan manusia, termasuk dalam sektor keuangan, yang menghasilkan inovasi dalam layanan

keuangan berbasis teknologi informasi yang sering disebut sebagai *financial technology* atau fintech. Salah satu *E-wallet* yang sedang berkembang adalah OVO, yang menawarkan uang elektronik dan poin untuk berbelanja di berbagai merchant yang menerima OVO. Untuk mengurangi risiko seperti *malfunction,* OVO bermitra dengan *CashShield*, sebuah perusahaan yang mengkhususkan diri dalam mengatasi penipuan dan pencurian, untuk meningkatkan keamanan sistem OVO dan melindungi data pengguna. Layanan *fintech* seperti *E-wallet* adalah bisnis yang membutuhkan kepercayaan karena melibatkan dana konsumen yang dikelola dalam platform digital. Sehingga penting untuk memperkuat sistem keamanan demi membangun kepercayaan pengguna terhadap keamanan dana dan data. *E-wallet* sama seperti dompet fisik dan digunakan untuk menyimpan informasi seperti nomor kartu kredit, *e-money*, identitas pemilik, dan informasi kontak. Pada penggunaan *E-wallet*, konsumen hanya perlu memasukkan informasi sekali dan dapat menggunakannya untuk bertransaksi di berbagai situs web. [12]

Penggunaan *mobile payment* di Indonesia dimulai sejak awal tahun 2000-an. *Mobile Payment* memberikan kemudahan kepada pengguna untuk melakukan transaksi keuangan melalui perangkat mobile, sejalan dengan perkembangan teknologi, muncul juga potensi risiko dan ancaman baru terkait dengan penggunaan mobile payment. Aplikasi mobile payment bisa disalahgunakan untuk melakukan tindakan kejahatan seperti pencucian uang dan akses ilegal ke informasi pribadi. *Mobile payment* menjadi tantangan baru bagi penegak hukum dalam menemukan bukti terkait dengan tindakan kejahatan yang melibatkan penggunaan aplikasi ini. Proses analisis forensik *mobile* menjadi sangat penting dalam menangani kasus-kasus tindak kejahatan yang melibatkan mobile payment. Melibatkan pengumpulan, analisis, dan dokumentasi artefak digital dari perangkat *mobile* yang dapat digunakan sebagai bukti dalam proses hukum. *Mobile* forensik adalah bagian penting dari ilmu digital forensik yang memainkan peran kunci dalam memeriksa dan memastikan keabsahan bukti digital dalam proses penegakan hukum. Hasil analisis *mobile* forensik dapat dijadikan

sebagai barang bukti yang sah dalam pengadilan dan membantu dalam penegakan hukum yang efektif.[13]

Kemajuan teknologi, terutama dalam Sistem Pembayaran Elektronik (SPE), terus mengalami pertumbuhan yang signifikan, baik dari segi nilai maupun volume transaksi. SPE telah berkembang pesat dalam dekade terakhir, namun kekhawatiran terkait keamanan dan kepercayaan masih ada, dan ini tetap menjadi perhatian di tahun 2000-an. Pada konteks SPE, keamanan diartikan sebagai serangkaian langkah, mekanisme, dan program komputer yang digunakan untuk mengotentikasi sumber informasi serta menjaga integritas dan privasi data tersebut. Kepercayaan adalah elemen kunci dalam hubungan transaksional, terutama dalam transaksi online yang sering kali memiliki tingkat risiko tinggi. Kurangnya rasa aman dan kepercayaan dapat menjadi penghambat perkembangan *E-commerce*.[14]

Aplikasi Android memiliki kemampuan untuk berinteraksi satu sama lain dan bertukar pesan untuk memberikan layanan melalui sistem penyampaian pesan Android. *Malware* seperti virus, Trojan, dan alat mata-mata membawa ancaman serius terhadap perangkat seluler, termasuk risiko bocornya informasi pribadi, potensi kerugian finansial, pengurasan daya baterai, dan penurunan kinerja jaringan. Pengujian penetrasi, yang juga dikenal sebagai *Pen-test*, berperan dalam mengidentifikasi kerentanan dalam aplikasi dengan menghadirkan skenario pengujian yang mengungkapkan potensi masalah yang dapat dimanfaatkan oleh penyusup untuk mendapatkan akses ke data atau sistem*. Pen-testing* biasanya dilakukan saat penerapan aplikasi dan tidak harus dilakukan pada setiap tahap siklus pengembangan perangkat lunak. Kekurangan dalam pengujian keamanan pasca penerapan, serta kurangnya pengujian regresi, dapat mengakibatkan kesalahan tambahan dan menjadikan aplikasi rentan. Ketidakmampuan melakukan pengujian penetrasi oleh pengembang aplikasi seluler juga dapat menyebabkan aplikasi tersebut menjadi tidak aman. Peretas etis juga dapat melakukan pengujian penetrasi dengan izin pemilik sistem untuk mengidentifikasi dan memanfaatkan

kerentanan dalam sistem. Jenis peretasan ini dianggap sah karena kerentanan yang ditemukan biasanya dilaporkan kepada pemilik sistem untuk perbaikan. Kerentanan keamanan tetap menjadi masalah, dan aplikasi dapat menjadi pintu masuk bagi serangan berdasarkan perilakunya termasuk aplikasi seperti *spyware*, yang dapat mengirimkan data ke tujuan yang tidak sah dan memantau perilaku pengguna, serta perangkat lunak seluler yang tidak diinginkan, yang dapat mengumpulkan informasi tentang *file*, akun, dan informasi perangkat lain tanpa izin pengguna.[15]

1.2 Identifikasi Masalah

Dilihat dari latar belakang yang telah diuraikan dapat diidentifikasi masalah yang dijadikan bahan penelitian terdapat celah keamanan yang masih ada dan dapat disalahgunakan oleh oknum yang tidak bertanggung jawab untuk mengambil keuntungan pribadi.

1.3 Batasan Masalah

Agar penyusunan penelitian ini tidak keluar dari topik permasalahan yang telah dirumuskan, maka ruang lingkup pembahasan dibatasi dengan:

1) Vmos Pro 2.3.4
2) Kopi Kenangan 122.06.24
3) Android Nougat 7.0

1.4 Rumusan Masalah

Berdasarkan latar belakang masalah diatas, maka dapat dirumuskan beberapa masalah antara lain:

1) Bagaimana cara agar promo pengguna baru tidak disalahgunakan lagi ?
2) Bagaimana cara agar aplikasi Kopi Kenangan dapat mendeteksi perangkat yang tidak sesuai dengan ketentuan promo yang telah ditetapkan ?
3) Bagaimana tahapan aplikasi mendeteksi pemakaian tidak wajar ?

1.5 Tujuan Penelitian

Tujuan penelitian yang ingin dicapai sebagai berikut:

1) Bertujuan untuk mengetahui tingkat keamanan pada aplikasi Kopi Kenangan sudah sampai tahap mana.
2) Bertujuan untuk mengetahui dampak dari pembuatan akun baru secara berulang-ulang dalam satu perangkat.
3) Bertujuan agar kemanan pada aplikasi Kopi Kenangan dapat ditingkatkan keamanan nya dan bisa mendeteksi perbedaan perangkat modifikasi dengan perangkat bawaan pabrik.

1.6 Manfaat Penelitian

Manfaat yang diperoleh dari penelitian ini antara lain :

1) Meningkatkan keamanan pada aplikasi Kopi Kenangan.
2) Sebagai pencegahan tindak *Cyber Crime*.
3) Menambah refrensi untuk peneliti dan peneliti selanjutnya.