BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi digital telah mendorong adopsi perangkat *mobile* secara masif di berbagai sektor kehidupan. Di Indonesia, 98,7% masyarakat berusia di atas 16 tahun mengakses internet melalui ponsel [1]. Data terbaru dari *Survei* Internet Indonesia 2024 yang dilakukan oleh APJII menunjukkan bahwa sebanyak 99,51% pengguna internet di Indonesia mengakses internet menggunakan perangkat *handphone* atau tablet, sementara hanya 0,88% menggunakan komputer atau laptop, dan 9,68% menggunakan keduanya [2].

Dominasi ini turut mendorong transformasi digital di berbagai sektor, termasuk industri kelapa sawit, yang merupakan komoditas penting bagi perekonomian Indonesia. Berdasarkan data GAPKI pada Januari 2025, volume ekspor minyak sawit Indonesia tercatat sebesar 1,96 juta ton, dengan ekspor *CPO* mencapai 39.000 ton pada bulan pertama tahun ini [3]. Untuk meningkatkan efisiensi dan akurasi operasional, telah dikembangkan sebuah aplikasi *mobile* sistem informasi panen sawit (*sawitgodigi.apk*, versi 1.0.0) berbasis *Android*, yang memungkinkan pencatatan hasil panen dilakukan secara digital melalui perangkat *mobile*. Namun, di balik inovasi tersebut, muncul tantangan serius terkait keamanan informasi, terutama karena aplikasi ini menangani data strategis seperti jumlah hasil panen, lokasi kebun, dan identitas pengguna.

Laporan Zimperium 2025 *Global Mobile Threat Report*, menyebutkan bahwa 25,3% perangkat *mobile* di dunia masih menggunakan sistem operasi yang tidak mendapat pembaruan keamanan, sehingga rentan terhadap *eksploitasi*. Selain itu, 23,5% perangkat *enterprise* mengandung aplikasi hasil *sideloading* yang sering dimodifikasi untuk tujuan jahat, seperti pencurian data atau pengambilalihan sistem. Kondisi ini semakin diperparah ketika aplikasi disebarluaskan melalui jalur informal, misalnya penginstalan manual via *Apk*, yang kerap terjadi di lapangan [4].

Di sisi lain, lebih dari 60% aplikasi *IOS* dan 34% aplikasi *Android* diketahui tidak memiliki perlindungan kode dasar seperti teknik *obfuscation*, enkripsi lokal, dan proteksi *runtime*, yang membuka peluang besar bagi tindakan *reverse engineering* dan penyisipan *malware* pada aplikasi yang seolah-olah sah. Masalah serupa juga terjadi dalam aspek komunikasi jaringan [4]. Laporan dari *ASEE* menunjukkan bahwa kurangnya enkripsi *end-to-end* serta tidak digunakannya validasi sertifikat *SSL* membuka potensi terjadinya serangan seperti *Man-in-the-Middle (MITM)* dan *network spoofing* [5].

Permasalahan ini menjadi sangat relevan dalam konteks pengembangan aplikasi sistem informasi panen sawit (*sawitgodigi.apk*, versi 1.0.0), yang saat ini masih berada dalam tahap pengembangan dan belum dirilis secara publik. Tanpa pengujian keamanan yang memadai, aplikasi ini sangat rentan dimanfaatkan oleh pihak tidak berwenang, sehingga dapat membahayakan data strategis, mengganggu proses operasional, dan merusak kepercayaan pengguna terhadap sistem digital yang dikembangkan.

Sebagai upaya mitigasi risiko, penelitian ini mengusulkan pendekatan pengujian keamanan dengan mengintegrasikan dua metode utama, yaitu analisis statis dan analisis dinamis menggunakan *Mobile Security Framework (MobSF)*. Analisis statis dilakukan terlebih dahulu terhadap file *APK* untuk mengidentifikasi kerentanan pada struktur internal aplikasi, seperti izin akses, konfigurasi *manifest*, dan penggunaan pustaka pihak ketiga [6]. Berdasarkan hasil temuan tersebut, dilakukan perbaikan awal terhadap komponen yang teridentifikasi rentan, sebelum aplikasi diuji lebih lanjut melalui analisis dinamis. Pada analisis dinamis, aplikasi dijalankan di dalam emulator *Android* yang telah di-root untuk mengamati perilaku aplikasi secara runtime, seperti lalu lintas jaringan, interaksi *API*, hingga aktivitas mencurigakan yang mungkin tidak terdeteksi saat analisis statis [7].

Penelitian ini memiliki kesamaan metodologi dengan studi yang dilakukan oleh Sabrina Uhti Kusreynada dan Azhari Shouni Barkah (2024) berjudul "*Android Apps Vulnerability Detection with Static and Dynamic Analysis Approach using MobSF*". Penelitian tersebut menganalisis aplikasi *Mobile* JKN milik BPJS Kesehatan yang sempat mengalami insiden kebocoran data. Para peneliti berhasil mengidentifikasi

berbagai kerentanan seperti penggunaan algoritma kriptografi yang usang, *hardcoded credentials*, serta serangan jenis *SQL Injection* dan *Janus*. Meskipun aplikasi telah menerapkan *SSL Pinning*, studi tersebut menunjukkan bahwa celah keamanan masih terbuka, terutama pada perangkat yang telah di-root dan dalam kondisi *debugging* aktif [8]

Berbeda dari studi sebelumnya yang hanya bersifat mendeskripsikan kerentanan, penelitian ini tidak hanya bertujuan menganalisis, tetapi juga memperbaiki temuan yang dihasilkan dari analisis statis sebelum dilanjutkan ke tahap dinamis. Evaluasi menyeluruh dilakukan terhadap hasil dari kedua tahap untuk menilai efektivitas perbaikan serta ketahanan sistem terhadap ancaman keamanan yang potensial. Dengan pendekatan sistematis ini, penelitian diharapkan mampu mengidentifikasi serta memitigasi potensi risiko keamanan sejak tahap awal pengembangan.

1.2 Rumusan Masalah

Pesatnya adopsi aplikasi *mobile* dalam berbagai sektor telah memberikan kontribusi besar terhadap efisiensi layanan digital, termasuk dalam bidang pertanian. Salah satu implementasinya adalah pengembangan aplikasi *mobile* sistem informasi panen sawit (*sawitgodigi.apk*, versi 1.0.0) yang dirancang untuk mencatat hasil panen secara digital melalui perangkat seluler langsung di lapangan.

Dalam praktik pengujian keamanan aplikasi *mobile*, dua pendekatan utama yang umum digunakan adalah analisis statis dan analisis dinamis. Analisis statis dilakukan tanpa mengeksekusi aplikasi, dengan menelaah elemen internal seperti konfigurasi *manifest*, izin akses *(permissions)*, dan pustaka pihak ketiga. Sementara itu[6], analisis dinamis dijalankan pada lingkungan virtual *(emulator)*, guna memantau perilaku aktual aplikasi, termasuk lalu lintas jaringan, pemanggilan *API*, dan interaksi terhadap sistem secara *real-time* [7].

Mobile Security Framework (MobSF) merupakan salah satu alat pengujian keamanan yang mengintegrasikan kedua pendekatan tersebut secara terpadu [9]. Namun, hingga kini masih sedikit penelitian yang secara sistematis memanfaatkan kedua pendekatan secara berurutan dan membandingkan hasilnya secara menyeluruh. Terlebih lagi, kontribusi berupa perbaikan sistem berdasarkan hasil

temuan analisis statis dan dampaknya terhadap hasil analisis dinamis masih jarang dibahas secara eksplisit.

Berdasarkan hal tersebut, penelitian ini difokuskan untuk menjawab pertanyaan berikut :

1. Bagaimana analisis keamanan dilakukan terhadap aplikasi *mobile* sistem informasi panen sawit (*sawitgodigi.apk*, versi 1.0.0) menggunakan pendekatan analisis statis dan analisis dinamis melalui *Mobile Security Framework (MobSF)*?
2. Sejauh mana perbaikan yang dilakukan terhadap temuan dari analisis statis mempengaruhi hasil analisis dinamis, dan bagaimana kedua pendekatan tersebut saling melengkapi ketika dibandingkan hasil temuan keduanya?

1.3 Batasan Masalah

Batasan masalah dalam penelitian ini difokuskan pada pengujian aspek keamanan terhadap aplikasi *mobile* Sistem Informasi Panen Sawit (*sawitgodigi.apk*, versi 1.0.0) berbasis *Android*. Pengujian keamanan dilakukan dengan memanfaatkan *Mobile Security Framework (MobSF)* melalui dua pendekatan utama, yaitu analisis statis dan analisis dinamis. Penelitian ini tidak mencakup penggunaan metode pengujian keamanan lain di luar *Mobile Security Framework (MobSF)* serta tidak membahas aspek keamanan yang berada di luar cakupan pendekatan analisis statis dan analisis dinamis yang digunakan, termasuk pengujian keamanan terhadap kode sumber *backend* secara langsung.

1.4 Tujuan

Adapun tujuan yang ingin dicapai dalam penelitian ini adalah sebagai berikut:

1. Melakukan analisis keamanan terhadap aplikasi *mobile* sistem informasi panen sawit (*sawitgodigi.apk*, versi 1.0.0) menggunakan pendekatan analisis statis dan analisis dinamis melalui *Mobile Security Framework (MobSF)*.
2. Mengevaluasi pengaruh perbaikan terhadap temuan analisis statis terhadap hasil analisis dinamis, serta menganalisis sejauh mana kedua pendekatan tersebut saling melengkapi berdasarkan perbandingan hasil temuan yang diperoleh.

1.5 Manfaat

Adapun manfaat yang diharapkan dari penelitian ini adalah sebagai berikut :

1. Secara teoretis, memberikan kontribusi ilmiah dalam bidang pengujian keamanan aplikasi *mobile* melalui kombinasi analisis statis dan dinamis menggunakan *Mobile Security Framework (MobSF)*.
2. Secara teoretis, menjadi referensi metodologis bagi penelitian sejenis dalam evaluasi dan perbaikan kerentanan aplikasi *mobile* berbasis *Android*.
3. Secara praktis, membantu pengembang dalam mengidentifikasi dan memperbaiki kerentanan pada aplikasi *mobile* sistem informasi panen sawit (*sawitgodigi.apk*, versi 1.0.0) sebelum dirilis.
4. Secara praktis, menyediakan rekomendasi teknis untuk meningkatkan keamanan aplikasi mobile di sektor perkebunan atau layanan digital sejenis.

1.6 Sistematika Penulisan

Sistematika penulisan dalam skripsi ini meliputi lima bab, yaitu :

Bab 1 Pendahuluan

Bab ini membahas latar belakang penelitian, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian, serta sistematika penulisan skripsi.

Bab 2 Tinjauan Pustaka

Bab ini memuat kajian terhadap penelitian terdahulu yang relevan serta landasan teori yang mendukung penelitian.

Bab 3 Metode Penelitian

Bab ini menjelaskan metode penelitian yang digunakan, meliputi data dan alat penelitian, prosedur penelitian, analisis kebutuhan, serta perancangan penelitian yang dilakukan.

Bab 4 Hasil dan Pengujian

Bab ini menyajikan hasil penelitian, pelaksanaan pengujian, data hasil pengujian, serta analisis dan evaluasi terhadap data hasil penelitian.

Bab 5 Penutup

Bab ini memuat kesimpulan dan saran berdasarkan hasil penelitian yang telah dilakukan.