BAB I
PENDAHULUAN

1.1 Latar Belakang

Pertumbuhan pesat aplikasi *mobile*, terutama media sosial, terus meningkat pesat dan menjadi elemen penting dalam aktivitas digital masyarakat masa kini. Banyaknya pengguna serta tingginya intensitas pertukaran data menjadikan aplikasi *mobile* rentan terhadap berbagai ancaman keamanan. Beberapa studi menunjukan bahwa aplikasi *android* sering memiliki kekurangan keamanan seperti izin yang tidak tepat, kebocoran data dan komunikasi yang tidak aman [1].

Dalam konteks yang lebih khusus aplikasi media sosial adalah jenis aplikasi dengan aliran data tertinggi yang dapat menyimpan dan memproses informasi sensitif pengguna. Hal ini meningkatkan kemungkinan terjadinya pencurian data, penyalahgunaan privasi, serta eksploitasi fungsi aplikasi. Fedynyshyn dan Partyka [9] menyatakan bahwa analitik aplikasi *mobile* sering kali mengumpulkan data pengguna dalam jumlah besar yang menyebabkan tantangan privasi dan keamanan yang signifikan dalam ekosistem saat ini.

Masalah utama yang dihadapi adalah banyaknya aplikasi *mobile* yang belum memenuhi standar keamanan baik secara statis maupun dinamis. Alviansyah dan Ramadhani [6] menyatakan bahwa dalam pengujian dinamis banyak aplikasi *android* tidak berhasil menangani kelemahan seperti autentikasi yang tidak aman dan kerentanan yang berbasis interaksi. Hal serupa terungkap dalam pengujian statis di mana aplikasi sering kali memiliki celah pada konfigurasi manifest, penggunaan izin yang berlebihan serta praktik penyimpanan data yang tidak aman [7].

Data empiris dari studi sebelumnya menegaskan betapa mendesaknya masalah ini. Abdillah, Trinoto dan himawan [3] mengidentifikasikan lebih dari 30 celah keamanan pada perangkat smart home yang berbasisi *android* dengan menggunakan *Mobile Security Framework* (*MobSF*). Dalam aplikasi e-commerce

Hanifurohman dan Hutagalung [8] juga mengidentifikasi berbagai risiko privasi dan konfigurasi yang berbahaya melalui analisis statis *MobSF*. Rejeki [4] menemukan kelemahan penting dalam aplikasi Kesehatan SatuSehat melalui analisis statis dan dinamis yang menunjukan risiko kebocoran data pengguna.

Secara teori evaluasi keamanan aplikasi *android* dapat dilakukan dengan dua pendekatan utama, analisis statis dan analisis dinamis. Analisis statis memusatkan perhatian pada evaluasi struktur aplikasi, izin Pustaka dan kode tanpa perlu menjalankan aplikasi [3]. Sebaliknya analisis dinamis menilai perilaku aplikasi selama eksekusi untuk mendeteksi interaksi yang mencurigakan, kebocoran data dan komunikasi yang tidak aman [6]. Keduanya menjadi elemen krusial dalam menilai Tingkat keamanan aplikasi media sosial.

Walaupun telah dilakukan banyak studi mengenai analisis kemanan aplikasi *mobile* dengan *MobSF*, mayoritas penelitian hanya menitikberatkan pada aplikasi tertentu seperti *e-commerce* dan lebih sering menggunakna satu metode analisis, baik hanya statis atau dinamis. Studi komparatif mengenai analisis statis dan dinamis dalam kategori alikasi media sosial masih sedikit. Nurindahsari dan Zen [2] hanya menekankan analisis statis pada aplikasi streaming video, sedangkan Himawan, Septianzah dan Setiadi [5] berfokus pada analisis *malware* yang bersifat statis analisis tanpa membandingkan kedua metode tersebut. Inilah ruang lingkup penelitian yang masih sedikit diteliti.

Seiring meningkatnya kompleksitas aplikasi media sosial berbasis Android, metode pengujian keamanan konvensional menjadi kurang efektif dalam mengidentifikasi kerentanan secara menyeluruh. Menurut (Privacy and online social network. 2023) Aplikasi media sosial tidak hanya mengandung struktur kode yang kompleks, tetapi juga melibatkan komunikasi jaringan yang intens, penggunaan API eksternal, serta pemrosesan data pribadi secara real time. Kondisi ini menimbulkan tantangan dalam mendeteksi kerentanan keamanan, khususnya yang berkaitan dengan kelemahan kriptografi, penyalahgunaan permission, dan potensi kebocoran data yang tidak selalu terlihat melalui pengujian manual atau satu pendekatan analisis saja.

Dalam konteks permasalahan tersebut, penggunaan Mobile Security Framework (MobSF) menjadi sangat mendesak karena mampu menyediakan mekanisme pengujian keamanan yang komprehensif melalui analisis statis dan dinamis secara terintegrasi. MobSF memungkinkan peneliti untuk mengidentifikasi kerentanan pada level kode, konfigurasi, serta perilaku aplikasi saat dijalankan, sehingga dapat memberikan gambaran tingkat keamanan aplikasi secara lebih akurat dan objektif [27]. Oleh karena itu, pemanfaatan MobSF dalam penelitian ini menjadi solusi yang relevan dan strategis untuk menjawab permasalahan keamanan aplikasi media sosial, sekaligus mendukung upaya peningkatan perlindungan data pribadi pengguna.

Berdasarkan penjelasan tersebut, penelitian ini bertujuan menganalisis serta membandingkan kemanan aplikasi media sosial dengan menggunakan metode analisis statis dan dinamis pada *Mobile Security Framework* (*MobSF*). Menurut (We Are Social & Meltwater. 2024) aplikasi Instagram, Facebook, dan TikTok sebagai objek penelitian didasarkan pada tingkat popularitas dan jumlah pengguna yang sangat tinggi secara global maupun nasional. Berdasarkan laporan ketiga aplikasi tersebut secara konsisten menempati peringkat teratas sebagai aplikasi media sosial yang paling banyak digunakan, khususnya pada platform Android. Tingginya jumlah pengguna menunjukkan besarnya volume data yang diproses dan dipertukarkan oleh aplikasi, sehingga meningkatkan potensi risiko keamanan dan privasi data pengguna. Studi ini diharapkan dapat memberikan konstribusi empiris untuk memperkuat pemahaman tentang keefektifan kedua pendekatan dalan mengidentikfikasi kerentanan pada aplikasi media sosial yang memiliki risiko kemanan tinggi.

1.2 Rumusan Masalah

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

1. Bagimana Tingkat keamanan aplikasi media sosial Instagram, Facebook dan Tiktok berdasarkan hasil analisis statis dan dinamis menggunakan *Mobile Security Framework* (*MobSF*)?

2. Jenis-jenis kerentanan apa saja yang terdeteksi melalui analisis statis dan dinamis pada ketiga aplikasi media sosial tersebut?
3. Bagaimana perbandingan keamanan antara analisis statis dan dinamis pada aplikasi media sosial tersebut?

1.3 Batasan Masalah

Batasan masalah yang digunakan untuk mempersempit permasalahan yang diangkat pada skripsi ini diberikan batasan-batsan yaitu:

1. Menggunakan *Mobile Security Framework* (*MobSF*) sebagai *Framework* pendeteksi keamanan aplikasi *android* yang digunakan.
2. Penilaian tingkat kerentanan hanya menggunakan indikator dan metrik yang disediakan oleh *MobSF*.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Untuk kemajuan dan pengembangan ilmu pengetahuan.
2. Mengetahui celah kemanan dari aplikasi *android* Instagram, Facebook dan TikTok yang didapatkan dari *Mobile Security Framework* (*MobSF*).

1.5 Manfaat Penelitian

Penelitian ini diharapkan mampu memberikan pemahaman dan meningkatkan kesadaran pengguna smartphone tentang kemungkinan risiko kemanan dari aplikasi media sosial yang mereka gunakan setiap hari. Pengguna dapat mengenali bagaimana kerentanan seperti permesion berbahaya, kebocoran data atau komunikasi yang tidak aman dapat memengaruhi keamanan data pribadi mereka.

1.6 Sistematika Penulisan

Sistematika penulisan skripsi ini disusun untuk memberikan gambaran yang terstruktur mengenai alur pembahasan penelitian dari awal hingga akhir. Adapun sistematika penulisan dalam skripsi ini adalah sebagai berikut:

BAB I Pendahuluan

Bab ini berisi latar belakang penelitian yang menguraikan alasan pemilihan topik keamanan aplikasi media sosial, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, serta sistematika penulisan skripsi

BAB II Tinjauan Pustaka dan Dasar Teori

Bab ini membahas kajian pustaka yang berkaitan dengan penelitian, meliputi penelitian-penelitian terdahulu, dasar teori mengenai keamanan aplikasi mobile, Mobile Security Framework (MobSF), analisis statis dan analisis dinamis, karakteristik aplikasi media sosial sebagai objek penelitian, serta gap penelitian dan kerangka pemikiran yang digunakan sebagai landasan teoritis penelitian.

BAB III Metode Penelitian

Bab ini menjelaskan metode penelitian yang digunakan, meliputi objek penelitian, alur penelitian, alat dan bahan, metode pengumpulan data, serta tahapan analisis statis dan dinamis menggunakan Mobile Security Framework (MobSF) dalam menguji keamanan aplikasi media sosial.

BAB IV Hasil dan Pembahasan

Bab ini menyajikan hasil analisis statis dan analisis dinamis terhadap aplikasi Instagram, Facebook, dan TikTok. Selain itu, dilakukan pembahasan serta perbandingan hasil pengujian dari kedua metode untuk menilai tingkat keamanan dan karakteristik kerentanan pada masing-masing aplikasi.

BAB V Kesimpulan dan Saran

Bab ini berisi kesimpulan yang diperoleh berdasarkan hasil analisis dan pembahasan penelitian, serta saran yang dapat dijadikan acuan untuk penelitian selanjutnya maupun pengembangan keamanan aplikasi media sosial di masa mendatang.