Analisis Keamanan Aplikasi Dompet Digital Pendekatan Statis dan Dinamis

Arya kukuh Yudatama[a], Indra Gunawan[b*],

[ab] Program Studi Informatika, Sekolah Tinggi Teknologi Ronggolawe Cepu
[*] Penulis Korenspondensi, Email: igunsttr@gmail.com

Diterima : 08-05-2023 - Direview : 23-05-2023 - Diterbitkan : 30-06-2023

Intisari

Aplikasi Android adalah aplikasi atau perangkat lunak yang menggabungkan fungsi-fungsi tertentu dengan cara yang dapat diakses oleh pengguna. Tujuan dari penelitian ini adalah untuk mengetahui tingkat keamanan aplikasi dompet digital DANA, OVO, GOPAY, Link aja dan Shopee Pay. Analisis yang digunakan meliputi dua metode yaitu analisis statis menggunakan MOBSF untuk menganalisis kode aplikasi, dan analisis dinamis menggunakan Wireshark dan Network Miner untuk memantau aplikasi ketika dijalankan. Hasil penelitian yang dilakukan dengan metode statis menghasilkan bahwa lima aplikasi dompet digital memiliki kerentanan. Sedangkan pada analisis metode dinamis tidak ditemukan kerentanan.

Kata kunci : Aplikasi android, Dompet digital, Digital Forensika, MOBSF, Network Miner.

Abstract

An Android application is an application or software that combines certain functions in a way that is accessible to the user. The purpose of this study is to determine the security tingkat of the DANA, OVO, GOPAY, Link aja and Shopee Pay digital wallet applications. The analysis used includes two methods, namely static analysis using MOBSF to analyze the application code, and dynamic analysis using Wireshark and Network Miner to monitor the application when it is running. The results of research conducted with static analysis show that five digital wallet applications have a vulnerabilites. Meanwhile, in the dynamic method analysis, no vulnerabilities were found.

Keywords : android application , digital wallet, digital forensics , MOBSF , Network minner.

1. Pendahuluan

E-wallet adalah layanan elektronik untuk menyimpan informasi tentang alat pembayaran, seperti B. Alat pembayaran dengan menggunakan kartu dan uang elektronik, yang dapat berisi dana untuk pembayaran. Tergantung dari harganya, layanan fintech (financial technology) berupa aplikasi e-wallet dapat memberikan kemudahan transaksi online dan offline yang dapat diakses melalui satu layanan yaitu aplikasi e-wallet. Berdasarkan data terbaru dari Internetworldstatis, terdapat 212,35 juta pengguna internet Indonesia pada Juni 2021. Hal ini menempatkan Indonesia pada urutan ketiga di Asia dengan pengguna internet terbanyak. Asia memiliki 2,77 miliar pengguna internet dari total populasi 4,33 miliar. Menurut Mobile Marketing Association (MMA), salah satu tren pengguna smartphone di Indonesia pada tahun 2021 adalah membayar layanan elektronik dengan dompet elektronik atau dompet digital. Berdasarkan data riset dari App Annie, tiga e-wallet bulanan teraktif di Indonesia adalah Gopay, OVO, dan DANA. Semakin berkembangnya dompet elektronik telah meningkatkan minat pengguna dompet elektronik di Indonesia, yang tidak terlepas dari manfaat praktis yang ditawarkan oleh layanan dompet digital.

Masyarakat Indonesia semakin meminta alat pembayaran yang tidak merepotkan, aman, nyaman dan mudah seperti dompet digital atau e-wallet sebagai alat pembayaran tunai. Menurut data Bank Indonesia (BI), nilai transaksi elektronik naik menjadi Rp19,2 triliun pada Februari 2021, naik 26 persen sehingga kebutuhan akan alat pembayaran digital juga semakin meningkat.

Menurut Divisi Cybercrime Badan Reserse Kriminal (Bareskrim) Kepolisian RI, penipuan digital menggunakan perangkat online merupakan salah satu bentuk kejahatan yang paling banyak terjadi. Jumlah total kejahatan dunia digital adalah 28,7 persen. Antara bulan Januari dan bulan September 2020, tercarat 649 laporan penipuan digital. Diantaranya meliputi 138 penggunaan data ilegal, 71 manipulasi data digital, dan 39 pencurian data digital dan atau identitas digital.

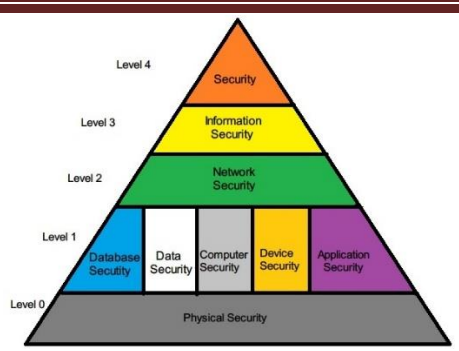
Oleh karena itu, perlu dilakukan analisis keamanan aplikasi dengan melakukan pengujian/pengukuran tingkat keamanan aplikasi. Mobile Security Framework (MobSF) dan Wireshark merupakan metode yang dapat digunakan untuk mengukur keamanan aplikasi.

2. Kerangka Teori

2.1. Tingkat Keamanan Perangkat

Tingkat Keamanan nol adalah keamanan pada area fisik atau dasar. Ketika area fisik terjaga, maka area internal perangkat juga terjaga. Perlindungan tingkat 1 terdiri dari perlindungan basis data, keamanan informasi, dan perlindungan perangkat. Pembuatan database menunjukkan apakah aplikasi yang diakui keamanannya digunakan. Selanjutnya, perhatian harus diberikan pada keamanan informasi, yaitu desain basis data, karena perancang basis data harus memikirkan kemampuan keamanan basis data. Yang terakhir adalah keamanan perangkat, yang digunakan untuk keamanan basis data.

Tingkat keamanan dua adalah keamanan informasi pada area jaringan. Tingkat keamanan tersebut merupakan kelanjutan dari keamanan tingkat pertama. Tingkat ketiga adalah keamanan pada area informasi. Informasi tersebut meliputi semua data pada sebuah perangkat. Tingkat keamanan tingkat empat adalah semua perlindungan tingkat satu hingga tingkat tiga. Jika salah satu tindakan pencegahan keamanan tidak terpenuhi pada tingkat dibawahnya, maka tingkat keamanan tingkat empat juga tidak terpenuhi. (A. Saya, 2013).



Gambar 2. 1 Tingkat Keamanan Smartphone

2.2. Dana

Berbasis di Jakarta, Indonesia, Dana adalah layanan keuangan digital yang bertindak sebagai mata uang digital untuk menggantikan dompet tradisional. Didirikan pada tahun 2018, DANA adalah dompet digital terdaftar Bank Indonesia dengan empat lisensi antara lain Uang Elektronik, Dompet Digital, Pengiriman Uang dan Likuiditas Keuangan Digital (LKD).

2.3 Ovo

OVO adalah aplikasi pembayaran serbaguna, sederhana, cepat dan aman yang siap membuat semua urusan keuangan Anda lebih nyaman. Sebanyak 58,9% responden pengguna dompet digital mengaku menggunakan OVO.

2.4 GO-PAY

GoPay adalah uang elektronik yang dapat Anda gunakan untuk pembayaran dan transaksi keuangan melalui aplikasi Gojek. GoPay memungkinkan Anda melakukan pembayaran ke Layanan Aplikasi GoPay, toko atau restoran, mitra bisnis GoPay, dan pelanggan PayLater. .

2.5 LINK AJA

LinkAja adalah layanan keuangan digital Telkomsel yang berbentuk uang elektronik milik BUMN. TCASH berfungsi seperti rekening bank yang fleksibel dan bebas bunga.Dengan

LinkAja, Anda dapat mengisi saldo hingga Rp2 juta, membayar berbagai tagihan, dan melakukan transaksi online dan offline melalui merchant rekanan. Layanan ini merupakan salah satu layanan dasar yang dapat digunakan oleh semua orang, termasuk pengguna baru

2.6 *Shopee Pay*

ShopeePay adalah layanan dompet digital yang disediakan oleh Shopee. ShopeePay menyatakan bahwa

frekuensi penggunaan platformnya akan meningkat dua kali lipat pada tahun 2021 dibandingkan tahun sebelumnya (kegembiraan). Penggunaan pembayaran digital saat ini semakin beragam. Mulai dari belanja makanan dan minuman, kebutuhan sehari-hari, produk atau layanan kesehatan, travel, fashion, kecantikan, hadiah, investasi, suplemen, hiburan, dan logistik. Peningkatan ini juga harus mencakup edukasi keselamatan saat menggunakan platform pembayaran digital.

2.7 *Software Wireshark*

Aplikasi wireshark adalah aplikasi yang dapat digunakan untuk menganalisis lalu lintas jaringan. Aplikasi Wireshark dapat menunjukkan secara detail lalu lintas jaringan sampai ke tingkat paket jaringan. Wireshark sendiri awalnya tidak didesain untuk para hacker/peretas. Fitur utama aplikasi Wireshark tidak ditujukan untuk hacking. Sebagai aplikasi utama para administrator jaringan, tugas utama aplikasi Wireshark adalah memantau lalu lintas jaringan yang lewat pada suatu perangkat yang sedang dianalisis.

2.8 MobSF

Mobile Security Framework(MobSF) merupakan aplikasi yang dapat digunakan untuk menganalisis paket aplikasi pada aplikasi-aplikasi android, biasanya memiliki format APK. Aplikasi MobSF dapat menampilkan pelaporan secara cepat dan efisien, juga lengkap. Aplikasi ini tersedia secara bebas dan bersifat online (Abraham, 2019).

2.9 Digital Forensics

Forensika digital adalah kegiatan investigasi secara digital untuk mencari bukti-bukti atau informasi digital yang digunakan untuk menguatkan atau memperlemah bukti fisik dari kasus yang sedang ditangani oleh pihak yang berwenang. Istilah forensika digital awalnya merupakan istiulah untuk forensika komputer. Istilah lalu menjadi lebih luas menjadi semua Teknik analisis pencarian bukti digital pada perangkat yang memiliki penyimpanan digital.

3.0 Analisis Metode Statis

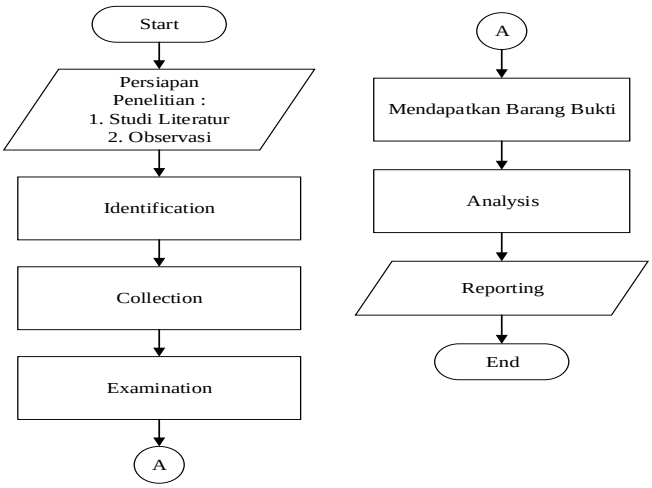
Analisis dengan metode statis adalah salah satu metode pengujian keamanan untuk menguji kode sumber aplikasi. Menurut (Hacken, 2019), MobSF adalah framework open source yang paling mudah digunakan dan nyaman serta tersedia secara online. Secara garis besar, analisis dengan menggunakan metode statis dengan MobSF meliputi:

1. Analisis metode enkripsi(SSL bypass)
2. Analisis Kelemahan kriptografi (Weak Crypto)
3. Analisis hak akses aplikasi (Permissions)
4. Analisis sisipan kode berbahaya(Hardcode secrets)
5. Analisis malware (Malware check)

3. Metodologi

3.1 Desain Peneitian

Bagan alir penelitian diperlukan untuk melakukan perencanaan proses, analisis proses dan dokumentasi proses sebagai panduan untuk melakukan penelitian. Berikut adalah diagram alir survei pada Gambar 3.1.



Gambar 3.1 Metode Penelitian

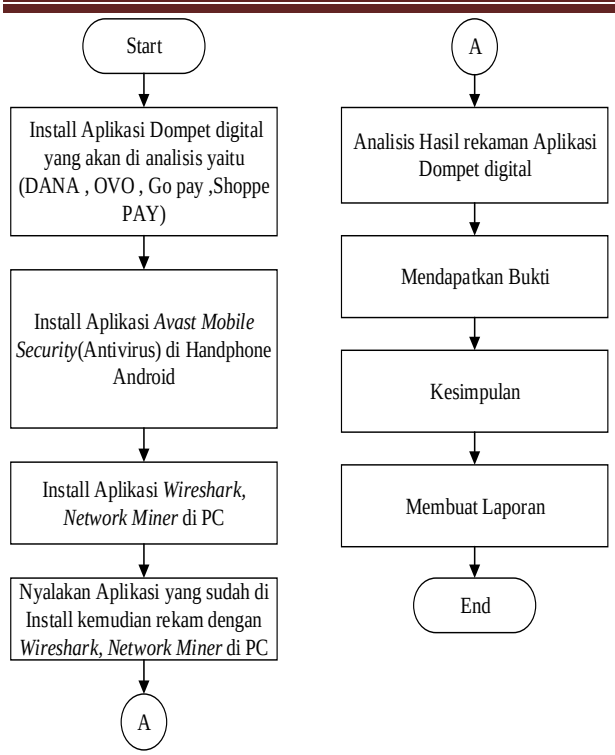
3.1.1 Metode Pengumpulan Data

Metode pengumpulan data pada penelitian ini antara lain:

a. Studi pustaka. Penulis studi literatur ini mengumpulkan sumber literatur dengan cara mencari informasi pada perpustakaan fisik maupun pada google scholar berkaitan dengan masalah yang diteliti.
b. Pengamatan. Pengamatan dilakukan menggunakan perangkat-perangkat digital dan menggunakan aplikasi pada skala laboratorium.

3.2 Metode Analisis

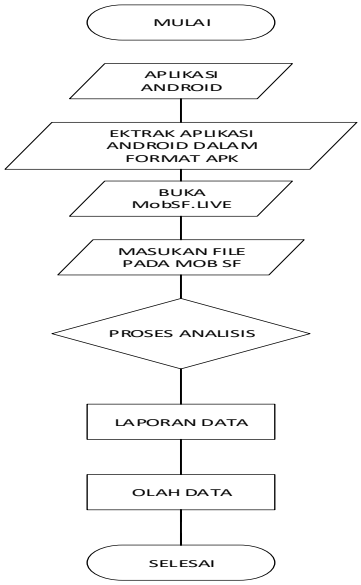
3.2.1 Metode Dinamis



3.2.1 Diagram Alir Analisis Dinamis

Metode dinamis adalah metode analisis dimana dilakukan analisis terhadap aplikasi yang sedang dijalankan.

3.3.1 Analisis Statis



Gambar 3.3.1 Flowchart Metode Statis

Metode statis adalah metode penganalisisan terhadap kode suatu aplikasi. Pada tahap ini perangkat lunak yang digunakan untuk melakukan analisis adalah MOBSF. Analisis metode statis yang dilakukan meliputi:

1. Analisis metode enkripsi(SSL bypass)
2. Analisis Kelemahan kriptografi (Weak Crypto)
3. Analisis hak akses aplikasi (Permissions)
4. Analisis sisipan kode berbahaya(Hardcode secrets)
5. Analisis malware(Malware check)

4. Hasil dan Pembahasan

4.1 Analisis Statis

Analisis menggunakan metode statis pada tahap ini dilakukan menggunakan aplikasi MobSF. Hasil dari tahap analisis statis tersebut dapat dilihat pada Tabel 4.2 dibawah ini.

4.4.1 Hasil Temuan Pada Aplikasi Dengan Metode Statis

Hasil Analisis Statis Aplikasi Dompet Digital								
NO	NAMA APLIKASI	WEAK CRYPTO	SSL Bypass	Dangerous permissions	Hardcode Secret	Root Detections	malware check	security score
1	OVO	YES	YES	YES	NO	YES	GOOD	47
2	GoPay	YES	YES	NO	NO	YES	GOOD	49
3	DANA	YES	YES	NO	YES	YES	GOOD	12
4	LinkAja	YES	YES	YES	NO	YES	GOOD	44
5	Shopee PAY	YES	YES	YES	YES	YES	GOOD	17

Tabel 4.1 Hasil analisis statis

4.2 Analisis Dinamis

Pada tahap ini, analisis dinamis dilakukan dengan menggunakan aplikasi antivirus Avast, Wireshark dan NetworkMiner. Aplikasi avast digunakan untuk mendeteksi kandungan malware. Aplikasi Wireshark digunakan untuk merekam lalu lintas jaringan, sedangkan aplikasi Network Miner digunakan untuk melakukan otomatisasi pelaporan aktifitas jaringan.

4.3 Tingkat Keamanan Aplikasi

Tingkat keamanan ini dapat dibagi menjadi beberapa tingkatan, yaitu: Keamanan tingkat nol adalah keamanan fisik atau dasar. Ketika keamanan fisik terjaga, keamanan internal smartphone juga terjaga. Perlindungan tingkat satu terdiri dari perlindungan basis data, keamanan informasi, dan perlindungan perangkat. Pembuatan database menunjukkan apakah aplikasi yang diakui keamanannya digunakan. Selanjutnya, perhatian harus diberikan pada keamanan informasi, yaitu desain basis data, karena perancang basis data harus memikirkan kemampuan keamanan basis data. Yang terakhir adalah perlindungan perangkat, yang

digunakan untuk keamanan basis data. Tingkat keamanan dua adalah keamanan informasi pada area jaringan. Perlindungan ini merupakan kelanjutan dari keamanan informasi tingkat satu. Tingkat tiga adalah keamanan pada area informasi. Tingkat keamanan empat adalah semua perlindungan tingkat satu sampai tingkat tiga. Jika salah satu tindakan perlindungan tidak terpenuhi, tingkat keamanan empat juga tidak terpenuhi. (Aku, 2013).

Tingkat Keamanan dari lima Aplikasi dompet digital adalah sebagai berikut :

1. OVO WhatsApp memiliki tingkat keamanan *Tingkat 4* dan menjadi peringkat ke 2
2. Go Pay memiliki tingkat keamanan *Tingkat 4* menjadi peringkat ke 1
3. DANA memiliki tingkat keamanan *Tingkat 4*. menjadi peringkat ke 5
4. Link Aja memiliki tingkat keamanan *Tingkat 4* menjadi peringkat ke 3
5. Shopee PAY memiliki tingkat keamanan *Tingkat 4* menjadi peringkat ke 4

5. Simpulan

Kesimpulan yang didapatkan pada penelitian ini adalah bahwa metode forensika digital dapat dilakukan untuk analisis keamanan pada aplikasi berbasis android. Metode statis dan dinamis digunakan untuk memastikan tidak ada celah keamanan pada area area kode aplikasi dan area jaringan.

Daftar Pustaka

Abraham, A. 2019. Mobile Security Framework Mobsf.

Deanna Durbin Hutagalung, & Cholis Hanifurohman. (2021). Analisis Statis Mengunakan Mobile Security Framework Untuk Pengujian Keamanan Aplikasi Mobile E- Comerce Berbasis Android. *SEBATIK 1410-3737*, 22-28.

Fianggara, A. Ji. (2018). No Title. Mahasiswa Universitas Brawijaya.

Gunawan, I. (2021) Keamanan Data: Teori Dan Implementasi. Sukabumi: Jejak.

Gunawan, I. (2021). Analisis Malware Botnet Proteus Pendekatan Static dan Dinamic. SIMETRIS, 15(1), 12-17

Gunawan, I. (2022). Analisis Keamanan Aplikasi Chat Android Pihak Ketiga Atau Non Playstore Menggunakan Digital Forensics. *SIMETRIS*, *16*(2), 1-6.

Http://Blog.Ub.Ac.Id/Jihadalif/2018/11/12/Ekonomi-Kelembagaandan-Pertumbuhan-Ekonomi/Karuniawan, M. I. (2016). *Penerapan Analisis Dinamis Untuk Pengujian Aplikasi Sia Umj Mobile*.

Kristianto, E. D. (2013).*Netminer, T O O L M O N I T O R I N G J A R I N G A N*.

Melania, D., & Gunawan, I. (2021). Analisis Keamanan Aplikasi Android Non Playstore Dengan Metode Digital Forensika Pendekatan Statis Dan Dinamis. *SIMETRIS, 15(2)*, 29-34.

Pranoto, W. (2018). Malicious Software Analysis . *Cybersecurity Dan Forensika Digital E-ISSN: 2615-8442* , 62-66.

Riadi, I., Umar, R., & Nasrulloh, I. M. (2018). *Analisis Forensika Digital Pada Frozen Solid State Drive Dengan Metode National Institute Of Justice (NIJ)*. *3*(May), 70–82.