Analisis Keamanan Data Pribadi pada Shopee Paylater Menggunakan Metode *Hybrid*

Nanang Widayanto*[1], Alfirna Rizqi Lahitani[2], Netania Indi Kusumaningtyas[3]
[1,2]Teknologi Informasi, FTTI Unjaya, Yogyakarta, Indonesia
[3]Sistem Informasi, FTTI Unjaya, Yogyakarta, Indonesia
e-mail: ***[1]nanangwidayanto1@gmail.com**, [2]alfirnarizqi@gmail.com, [3]netania0412@gmail.com

Abstract* - The low level of awareness and understanding of Shopee online shopping application users regarding the security of user data causes the level of digital crime to increase, as evidenced by the many crime cases that occur, namely the misuse of users' personal data by utilizing OTP codes as a verification process. This can be a loophole for digital crimes that are certainly very detrimental to users. Perform personal data security analysis on Shopee PayLater using the Hybrid method. The method used is the hybrid method, which is a method of combining basic digital forensic techniques with re-engineering techniques. This method can be used to analyze applications that involve user personal data, tools used such as MobSF, Virustotal to view application activity, and apk-deguard for apk reengineering. Personal data security research on Shopee PayLater was carried out using the help of Virustotal and MobSF tools found vulnerabilities caused by users. The results of the personal data security analysis carried out on the Android-based Shopee application show that there are several vulnerabilities in the user's personal data vulnerability, namely in the application licensing section.

Keywords *– MobSF, OTP, Personal Data, Shopee PayLater, Virustotal*

Abstrak* - Masih rendahnya tingkat kesadaran dan pemahaman pengguna aplikasi belanja online Shopee atas keamanan data pengguna menyebabkan tingkat kejahatan digital semakin bertambah, terbukti dengan masih banyaknya kasus kejahatan yang terjadi yaitu penyalahgunaan data pribadi pengguna dengan memanfaatkan kode OTP sebagai proses verifikasi. Hal ini dapat menjadi celah tindak kejahatan digital yang tentu sangat merugikan pengguna. Penelitian ini bertujuan untuk melakukan analisis keamanan data pribadi pada Shopee PayLater menggunakan metode Hybrid. Metode yang digunakan yaitu Metode hybrid ,merupakan metode penggabungan dari teknik dasar digital forensik dengan teknik Reengineering. Metode ini dapat di gunakan untuk menganalisis aplikasi yang melibatkan data pribadi pengguna, tool yang digunakan seperti MobSF, Virustotal untuk melihat aktifitas aplikasi, serta apk-deguard untuk re-engineering apk. Penelitian keamanan data pribadi pada Shopee PayLater dilakukan dengan menggunakan bantuan tool Virustotal dan MobSF ditemukan kerenatan yang diakibatkan oleh pengguna. Hasil analisis kemanan data pribadi yang dilakukan pada aplikasi Shopee berbasis android menunjukkan bahwa ada beberapa celah kerentanan data pribadi pengguna yaitu pada bagian perizinan aplikasi.

Kata kunci *- Data Pribadi, MobSF, OTP, Shopee PayLater, Virustotal*

I. PENDAHULUAN

Dalam perkembangan dunia digital, *e-commerce* telah menjadi cara transaksi yang populer bagi pelaku bisnis. Teknologi *e-commerce* memungkinkan pelaku bisnis untuk bertransaksi dengan para konsumen tanpa harus bertatap muka secara langsung karena sudah terjangkau oleh semua pengguna internet sehingga mempermudah para pelaku bisnis untuk memperluas jaringan pemasarannya. Namun, pertumbuhan *e-commerce* juga menghadirkan masalah kebocoran data pribadi yang perlu diperhatikan. Permasalahan ini sering kali di sepelekan oleh sebagian orang [1].

Shopee merupakan salah satu *platform e-commerce* yang banyak digunakan di Indonesia [2]. Menurut laporan data survei dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada tahun 2019 – 2020 menunjukkan bahwa Shopee merupakan *e-commerce* nomor satu yang banyak digunakan oleh masyarakat, dengan presentase 27,4%.

ShopeePay adalah fitur dompet digital di aplikasi Shopee yang menawarkan kemudahan pembayaran. Fitur Shopee PayLater merupakan inovasi keuangan yang memungkinkan pembayaran secara kredit tanpa jaminan yang bernilai besar dan tanpa membutuhkan kartu kredit mulai dari tempo 1 bulan hingga 12 bulan untuk berbelanja dengan suku bunga 0%-2,95%. Shopee PayLater bertujuan memenuhi kebutuhan masyarakat yang ingin berbelanja tetapi tidak memiliki cukup uang tunai. Pengguna Shopee PayLater hanya perlu mengajukan dengan foto KTP dan foto muka [3].

Namun, penggunaan kredit dalam sistem ini menimbulkan risiko keamanan data pribadi pengguna. Beberapa kasus penyalahgunaan data pribadi masih terjadi, terutama melalui penyalahgunaan kode OTP sebagai proses verifikasi. Oleh karena itu, diperlukan analisis terhadap kerentanan keamanan data pribadi dari sisi aplikasi Shopee untuk mengetahui ancaman yang terjadi kepada para pengguna aplikasi belanja online Shopee sehingga diharapkan dapat meningkatkan kesadaran dan pemahaman pengguna tentang keamanan data mereka.

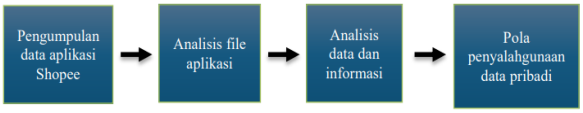
Terdapat beberapa penelitian analisis keamanan data yang relevan dengan topik yang dibahas. Penelitian dengan judul *Blockchain* Untuk Keamanan Transaksi

Elektronik Perusahaan *Financial* Teknologi membahas penggunaan teknologi *blockchain* untuk meningkatkan keamanan transaksi elektronik perusahaan *fintech* [4]. Penelitian kedua dengan judul Regulasi Keamanan Data Pribadi Pengguna Pada *E-commerce* di Indonesia mengulas regulasi keamanan data pribadi pengguna pada *e-commerce* di Indonesia [5]. Penelitian ketiga dengan judul Analisis Penyalahgunaan Data Pribadi Dalam Aplikasi *Fintech* Illegal Dengan Metode *Hybrid* menganalisis penyalahgunaan data pribadi dalam aplikasi *fintech* ilegal dan menggunakan metode *hybrid* [6]. Dari penelitian dengan judul Analisis Privasi Dan Kepercayaan Terhadap Keamanan Data Pengguna Aplikasi *On Demand Service* Menggunakan Metodologi *Structual Equation Modelling* menguji privasi dan kepercayaan terhadap keamanan data pengguna aplikasi *on-demand service* [7].

Dalam penelitian-penelitian ini, masalah yang diangkat meliputi rendahnya keamanan sistem, perlindungan data pribadi pengguna, penyalahgunaan data pribadi, dan kepercayaan pengguna terhadap keamanan aplikasi.

II. METODE PENELITIAN

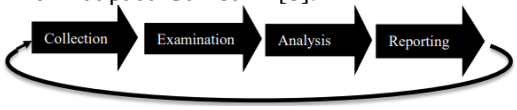
Metode yang digunakan untuk menganalisis keamanan data pribadi pada Shopee PayLater menggunakan metode *hybrid*. Alur metode penelitian ini ditujukan pada Gambar 1.



Gambar 1. Alur metode penelitian

Langkah-langkah analisis menggunakan metode *Hybrid*:

1. Pengumpulan data aplikasi Shopee, pengambilan dilakukan dengan cara mendownload aplikasi Shopee pada *smartphone* android di PlayStore.
2. Analisis *file* aplikasi, proses analisis dilakukan dengan menggunakan metode *hybrid*, yang didalamnya terdapat analisis statis dan analisis dinamis. Pada analisis statis, aplikasi langsung diinstal pada *smartphone* kemudian dilakukan analisis *interface* dan data yang dimasukkan. Pada analisis dinamis dilakukan dengan cara melakukan *re-engineeing source code* dan analisis keamanan proses berjalannya aplikasi Shopee serta aktivitas *malware*.
3. Analisis data dan informasi. Tahap ini dilakukan setelah *file* aplikasi ditemukan data-data dan informasi terkait penyalahgunaan data pengguna. Data pribadi pengguna yang diambil adalah data diri pada KTP. Pada tahap ini menggunakan metode NIST, ada 4 tahapan yang akan dilakukan, dapat dilihat pada Gambar 2 [8].



Gambar 2. Tahapan metode NIST

Terdapat 4 langkah untuk menganalisis keamanan data pribadi, yaitu :

1) *Collection*, merupakan tahapan paling awal dari metode NIST, hal-hal yang dilakukan dalam tahapan *collection* yaitu koleksi, dokumentasi, isolasi, preservasi dan preservasi barang bukti.
2) *Examination*, merupakan aktivitas *backup* data *smartphone* dapat menggunakan *tool* atau dicadangkan melalui pengaturan *smartphone*.
3) *Analysis*, merupakan proses untuk mendapatkan informasi yang berguna dan dapat menjawab apa yang dibutuhkan sebagai pendorong untuk melakukan pengumpulan dan pemerikasaan data.
4) *Reporting*, merupakan proses pelaporan dari hasil tahapan yang meliputi penjelasan mengenai alat yang digunakan, prosedur yang digunakan, penggambaran tindakan yang dilakukan, memberikan rekomendasi untuk perbaikan prosedur atau aspek lain pada aplikasi.

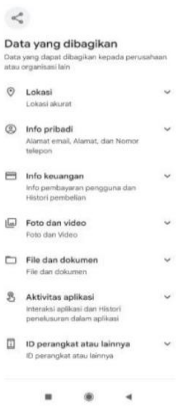
4. Pola penyalahgunaan data pribadi. Setelah ditemukan ciri-ciri pencurian data dan menyebarluaskan data pribadi pengguna, kemudian dikelompokkan yang kemudian dapat ditarik kesimpulan berupa pola penyalahgunaan data pribadi pengguna aplikasi Shopee.

III. HASIL DAN PEMBAHASAN

A. *Collection*

Tahapan paling awal dari metode NIST, hal-hal yang dilakukan dalam tahapan *collection* yaitu koleksi, dokumentasi, isolasi, preservasi dan preservasi barang bukti. Adapun langkah pada *Collection* sebagai berikut:

1. Menggunakan perangkat *smartphone* android Xiaomi.
2. Pengumpulan data aplikasi Shopee didapatkan dengan mengunduh aplikasi Shopee di PlayStore dengan *smartphone* android. Dapat dilihat pada Gambar 3 merupakan data yang dibutuhkan pada aplikasi. Dari uraian pada Gambar 3 dapat disimpulkan bahwa pengumpulan data yang dibutuhkan aplikasi Shopee adalah lokasi, informasi pribadi (berisi email, alamat pengguna, dan nomor telepon), info keuangan (berisi info pembayaran pengguna, dan riwayat pembelian), foto, *file* dan dokumen, aktivitas aplikasi (berisi interaksi aplikasi dan riwayat penelusuran pada aplikasi), dan ID perangkat.



Gambar 3. Data yang dibutuhkan pada aplikasi

B. Examination

Examination merupakan aktivitas *backup data smartphone* dapat menggunakan *tool* atau dicadangkan melalui pengaturan *smartphone*. *Backup* data *smartphone* android menggunakan fitur cadangkan dan setel ulang pada pengaturan *smartphone*. Hasil dari backup data *smartphone* ditempatkan pada penyimpanan *internal smartphone* yang dapat di salin pada *file explore* pada laptop.

C. Analysis

Analysis merupakan proses untuk mendapatkan informasi yang berguna dan dapat menjawab apa yang dibutuhkan sebagai pendorong untuk melakukan pengumpulan dan pemerikasaan data. Pada langkah ini terdapat 2 macam analisis yaitu analisis statis dan analisis dinamis.

1) Analisis Statis

Diawali dengan menginstal aplikasi ke *smartphone* android, kemudian data apa saja yang dimasukkan ke dalam aplikasi antara lain lokasi, informasi pribadi (berisi email, alamat pengguna, dan nomor telepon), info keuangan (berisi info pembayaran pengguna, dan riwayat pembelian), foto, *file* dan dokumen, aktivitas aplikasi (berisi interaksi aplikasi dan riwayat penelusuran pada aplikasi), dan ID perangkat, ditunjukkan pada Gambar 3. Adapun hasil analisis statis diperlukan untuk melihat sejauh mana aplikasi meminta data pengguna dalam proses membuat akun baru.

Tabel 1. Tabel analisis statis

No	Komponen	Data Aplikasi
1.	Pengembang	Shopee
2.	URL *web*	https://droidbang.com/files30/72474/com.shopee.id_2.92.08_667.apk/
3.	Nama *file*	Shopee ID Belanja Bebas Ongkir
4.	Ukuran *file*	230 MB
5.	Penggunaan data pribadi pengguna	Yang tercantum di KTP pengguna seperti: 1. NIK 2. Nama lengkap 3. Tempat/tgl lahir 4. Jenis kelamin 5. Alamat lengkap 6. Agama 7. Status perkawinan 8. Pekerjaan 9. Kewarganegaraan
6.	*File upload*	Foto muka dan foto KTP
7.	Media verifikasi	*Chat* WhatsApp

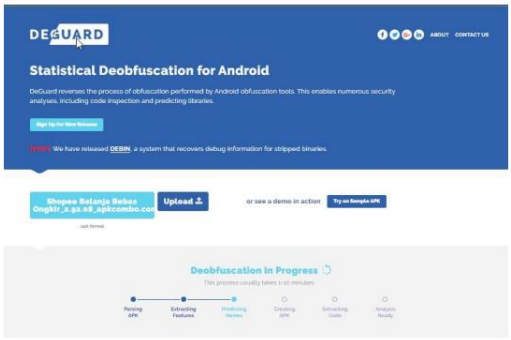
Dari hasil analisis statis pada Tabel 1 dapat ditarik kesimpulan bahwa terdapat data penting dan proses penting yang seharusnya melalui verifikasi dan dokumentasi. Kebijakan privasi dan penggunaan data merupakan hal pertama yang harus disiapkan oleh Shopee. Kebijakan ini merupakan sebuah perjanjian awal dalam penggunaan dan transaksi data informasi yang diberikan oleh calon penguna Shopee, dapat dilihat analisis diatas dalam mendaftar akun baru seseorang harus memasukkan data diri yang cukup lengkap yaitu dengan mengunggah foto KTP, hal tersebut akan berpengaruh terhadap kerahasiaan data pribadi terutama NIK.

2) Analisis Dinamis

Analisis dinamis dilakukan menggunakan dua cara, yang pertama yaitu menggunakan teknik *re-engineering file* apk, yang nantinya merubah *file* apk menjadi *file soure code* untuk dapat di analisis alur sistemnya. Untuk yang kedua yaitu dengan menggunakan teknik analisis proses genetik (*Genetic Malware Analysis*), teknik ini akan melihat proses apk apakah megandung aktifitas mencurigakan dalam pencurian data informasi atau tidak.

a) *Re-engineering file* apk

Tahapan proses *re-engineering file* apk menjadi *source code* dapat dilihat pada gambar dibawah ini yaitu dengan bantuan *tool* apk *deguard*



Gambar 4. Proses *re-engineering file* apk

Gambar 5. Hasil *re-engineering file* apk

Proses *Re-engineering file* apk Shopee dan hasil yang ditampilkan dapat dilihat pada Gambar 4 dan Gambar 5 ditunjukkan bahwa aplikasi *compatible* dengan versi minimal Android 7 dan untuk memverifikasi Shopee PayLater-nya dibutuhkan data dari KTP, dibutuhkan akses *proxy* untuk masuk ke dalamnya agar terhindar dari kerawanan data yang mudah terlacak.

b) Analisis Aktifitas Genetik

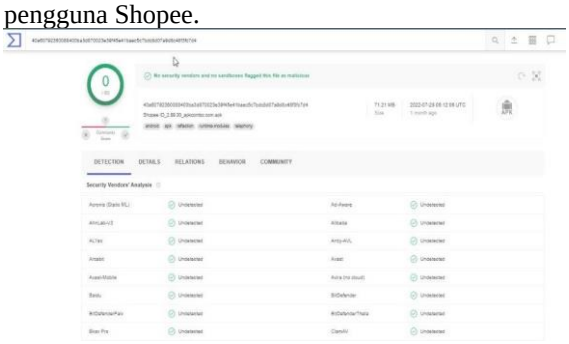
Analisis genetik dilakukan untuk melihat aktifitas yang menyerupai aktifitas *backdoor*, *malware* dan *virus*. Dimana aktifitas tersebut dapat memicu pencurian data. Analisis menggunakan *tool* Virustotal dan MobSF. selain itu dapat juga untuk melihat aktifitas yang dilakukan saat aplikasi dijalankan.

- Virustotal

Tampilan dari Virustotal dapat dilihat pada Gambar 6.

Gambar 6. Proses *upload file* aplikasi Shopee

Pada penelitian ini menggunakan *tool* Virustotal [9] untuk memindai data yang didapat dari perangkat *smartphone* yang ter-*install* aplikasi Shopee. Pada Gambar 6 menunjukkan bahwa untuk memindai data diperlukan proses *upload* untuk mendapatkan hasil dari pemindaian data pengguna Shopee.



Gambar 7. Hasil analisis *file* Shopee tampilan pertama

Berdasarkan analisis *file* aplikasi Shopee pada Gambar 7 dapat disimpulkan bahwa aplikasi dalam kondisi aman, tidak terdetekasi *malware* atau aktivitas berbahaya.

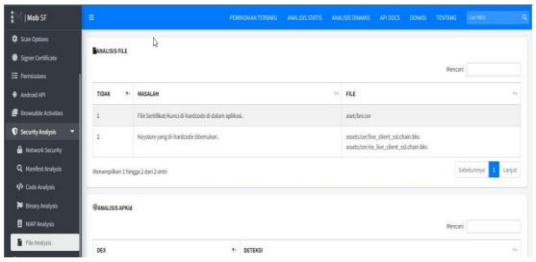
Gambar 8. Analisis pada perizinan aplikasi Shopee

Berdasarkan analisis *file* dalam bagian perizinan aplikasi pada Gambar 8 dijelaskan bahwa aplikasi dapat membaca dan menambahkan kalender pada Android, dapat menambah dan membaca memori *eksternal*, dapat membaca status telepon, dapat membaca daftar kontak yang tersimpan. Aktivitas ini dapat membuka informasi/berkas dari data pengguna Shopee.

- MobSF

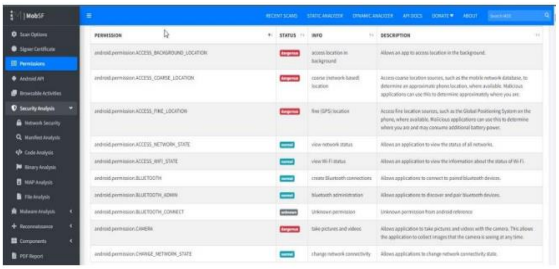
Analisis menggunakan *tool* MobSF untuk menganalisis aplikasi Shopee [10] mencakup *hardcode secrets, permisions dan malware check.* Dapat dilihat pada Gambar 9 merupakan proses *upload file* aplikasi Shopee.

Gambar 9. Proses *upload file* aplikasi Shopee



Gambar 10. Hasil analisis *file* Shopee

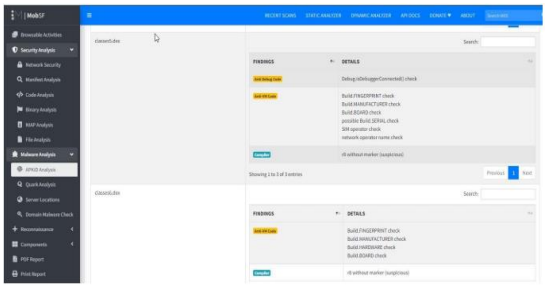
Pada analisis *file* Shopee pada Gambar 10 ditampilkan bahwa *file* aplikasi Shopee ada dua masalah pada *file* sertifikat/kunci di *hardcode* dalam aplikasi dan *keystore* yang di *hardcode* ditemukan.



Gambar 11. Hasil analisis pada perizinan aplikasi

Pada perizinan aplikasi pada Gambar 11 ditampilkan bahwa pada bagian *ACCES_BACKGROUND_LOCATION* yaitu mengizinkan aplikasi mengakses lokasi di latar belakang pada status bahaya, aktivitas tersebut sangat membahayakan data pribadi pengguna karena dapat membaca lokasi pengguna saat aplikasi tidak digunakan, pada bagian *ACCES_COARSE_LOCATION* berbahaya karena aplikasi dapat mengetahui keberadaan pengguna saat aplikasi digunakan, pada bagian *ACCES_FINE_LOCATION* yaitu jika lokasi terdeteksi bahwa jaringan GPS bagus maka aplikasi akan mengakses lokasi pengguna aplikasi dan hal tersebut dapat memperpendek penggunaan Andorid karena kehabisan baterai, pada bagian *CAMERA* yaitu mengizinkan aplikasi untuk mengakses foto dan video dari kamera Android,

aktivitas tersebut berbahaya karena dapat melihat gambar yang sudah tersimpan pada memori Android.



Gambar 12. Hasil analisis *malware*

Analisis *malware* pada Gambar 12 ditampilkan pada clasess5.dex dijelaskan bahwa ada hal yang mencurigakan yaitu pada *FINGERPRINT, MANUFACTURE, BOARD* yaitu pada *build serial*, SIM *operator*, dan jaringan *operator* karena pada fitur tersebut rawan pembobolan data pengguna karena mudah dalam melakukan eksekusi. Pada clasess 6 dijelaskan bahwa ada hal yang mencurigakan juga yaitu pada *FINGERPRINT, MANUFACTURE, HARDWARE*, dan *BOARD* karena pada fitur tersebut rawan pembobolan data pengguna.

Tabel 2. Tabel hasil analisis dinamis

No	Data/ Informasi	Hasil	Keterangan
1.	*Re-engineering file* apk *(apk-deguard)*	Menunjukkan bahwa aplikasi *compatible* pada versi Android minimal 7, untuk memverifikasinya dibutuhkan data pribadi pengguna dari KTP	Rawan terjadi pencurian data pribadi
2.	Aktivitas *genetic* (apk Virustotal)	Aplikasi Shopee tidak terdeteksi *Malware* berbahaya	Aman
3.	Aktivitas *genetic* (apk Mobsf)	Banyak fitur yang terdeteksi mencurigakan	Rawan terjadi pencurian data pribadi, maka dianjurkan pengguna agar lebih hati-hati

Dari Tabel 2 diketahui bahwa semua *tool* melakukan analisis aplikasi yang memberikan hasil masing-masing setiap langkah yang dilakukan. Sehingga dapat disimpulkan bahwa data informasi pengguna aplikasi yang tersimpan dalam Android dapat diakses oleh aplikasi deng mudah, jika diizinkan saat pertama membuat akun baru. Sehingga berpotensi data informasi yang seharusnya tidak dibutuhkan oleh aplikasi dapat ter-*input* dalam aplikasi.

D. Reporting

Proses pelaporan dari hasil tahapan yang meliputi penjelasan mengenai alat yang digunakan, prosedur yang digunakan, penggambaran tindakan yang dilakukan, memberikan rekomendasi untuk perbaikan prosedur atau aspek lain pada aplikasi.

Tabel 3. Hasil *reporting*

No	Tool	Langkah yang dilakukan	Kerawanan	Rekomendasi Solusi
1.	Apk deguard	*Scanning file* aplikasi Shopee	Pembobolan data pengguna dapat terjadi jika tidak adanya *proxy* khusus saat penggunaan aplikasi Shopee	Dibutuhkan akses *proxy* agar terhindar dari kerawanan data yang mudah terlacak oleh aplikasi Shopee
2.	Virusto-tal	*Scanning file* aplikasi Shopee	Jika tidak diizinkan saat bagian perizinan aplikasi untuk mengakses data pada smartphone maka aplikasi tidak terdeteksi kerawanan data yang mudah terlacak oleh aplikasi Shopee	Sebaiknya izinkan jika saat ingin digunakan saja seperti pembacaan kontak, kamera, dan yang lainnya
3.	MobSF	*Scanning file* aplikasi Shopee	Ada kecurigaan pembacaan data yang mengancam pembobolan data pribadi pengguna.	Sebaiknya lebih berhati-hati sebagai pengguna agar tidak terjadi pembobolan data pribadi

Dari hasil *reporting* yang di tampilkan pada Tabel 3 dapat disimpulkan bahwa setiap *tool* yang digunakan untuk analisis *file* memliki fungsi dan hasil yang berbeda serta didapatkan rekomendasi solusi supaya pengguna dapat memahami apa yang harus dilakukan supaya tidak terjadi kerentanan data pribadi yang tersebar.

IV. KESIMPULAN

Kesimpulan yang dapat diambil dari penelitian yang telah dilakukan diantaranya adalah hasil analisis kerentanan data pribadi yang dilakukan pada aplikasi Shopee menggunakan *tool* MobSF menunjukkan bahwa ada beberapa celah kerentanan data pribadi pengguna yaitu diantaranya pada aspek perizinan aplikasi, aspek keamanan aplikasi dan aspek analisis *malware*. Hasil

forensik kerentanan data pribadi pengguna aplikasi yang dilakukan analisis menggunakan *tool* Virustotal dihasilkan bahwa tidak ada hal mencurigakan pada aplikasi Shopee serta tidak terdeteksi *malware* yang mengancam data pribadi.

DAFTAR PUSTAKA

[1] S. W. Putra, "Aspek Cybercrime dalam Paylater," vol. 4, pp. 1–22, Mar. 2021.

[2] I. Saputra, G. M. A. Sasmita, and A. Wiranatha, "Pengembangan Sistem Keamanan untuk E-Commerce," *Jurnal Ilmiah Merpati (Menara Penelitian Akademika Teknologi Informasi)*, vol. 5, no. 1, p. 17, 2017.

[3] F. D. W. Damayanti and C. Canggih, "Pengaruh penggunaan pembayaran shopeepay later terhadap perilaku konsumsi islam generasi milenial di Surabaya," *Jurnal Ilmiah Ekonomi Islam*, vol. 7, no. 3, pp. 1905–1915, 2021.

[4] M. D. K. Perdani, W. Widyawan, and P. I. Santosa, "Blockchain untuk Keamanan Transaksi Elektronik Perusahaan Financial Technology (Studi Kasus pada PT XYZ)," *Semnasteknomedia Online*, vol. 6, no. 1, pp. 1–14, 2018.

[5] I. K. Noppi Adi Jaya and I. A. Utari Dewi, "Regulasi Keamanan Data Pribadi Pengguna pada E-commerce di Indonesia," 2022.

[6] H. Wijayanto, A. H. Muhammad, and D. Hariyadi, "Analisis Penyalahgunaan Data Pribadi Dalam Aplikasi Fintech Ilegal Dengan Metode Hibrid," *Jurnal Ilmiah SINUS*, vol. 18, no. 1, pp. 1–10, 2020.

[7] R. K. Novriantama, A. Kusyanti, and R. I. Rokhmawati, "Analisis Privasi dan Kepercayaan Terhadap Keamanan Data Pengguna Aplikasi On Demand Service Menggunakan Metodologi Structural Equation Modeling," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN*, vol. 2548, p. 964X, 2018.

[8] N. Nasirudin, S. Sunardi, and I. Riadi, "Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express," *Jurnal Informatika Universitas Pamulang*, vol. 5, no. 1, pp. 89–94, 2020.

[9] F. T. Saputra, B. Santoso, J. Kuswanto, and M. A. Ghofur, "Analisis Keamanan Informasi Kesadaran Pengguna WhatsApp Mod dengan Metode Analisis Statis dan Metode Kuantitatif," in *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia p-ISSN*, p. 5805.

[10] C. Hanifurohman and D. D. Hutagalung, "Analisa Keamanan Aplikasi Mobile E-Commerce Berbasis Android Menggunakan Mobile Security Framework," in *Seminar Nasional Enhancing Innovations for Sustainable Development*, 2020.