

PENGARUH PRIVASI DAN KEAMANAN TERHADAP PENGUNAAN MOBILE PAYMENT

Muhamad Badru Zaman¹, Ibrahim Bali Pamungkas², Wahyu Andri Wibowo³
Universitas Pamulang, Indonesia
dosen02589@unpam.ac.id¹, dosen01015@unpam.ac.id², dosen01908@unpam.ac.id³

Submitted: 17th July 2022/ **Edited:** 06th September 2022/ **Issued:** 01st October 2022
Cited on: Zaman, M. B., Pamungkas, I. B., & Wibowo, W. A. (2022). PENGARUH PRIVASI DAN KEAMANAN TERHADAP PENGUNAAN MOBILE PAYMENT. *SCIENTIFIC JOURNAL OF REFLECTION: Economic, Accounting, Management and Business*, 5(4), 891-902.

ABSTRACT

The purpose of this study was to determine how much positive and significant influence privacy and security partially or simultaneously on the performance of using mobile payment (Go-Pay). The object of this research is the students of Pamulang University Faculty of Economics and Business Management Study Program Level 1 users of mobile payment (Go-Pay). The type of research used in this research is descriptive quantitative. Methods of data collection using observation and questionnaires. The sampling technique used slovin with a number of respondents as many as 91 users. The validity of the data in this study used Validity Test, Reliability Test, and Classical Assumption Test. The result of this study is that there is a positive and significant influence partially or simultaneously between privacy and security on the use of mobile payment (Go-Pay).

Keyword : Privacy, Security, Mobile Payment Users

PENDAHULUAN

Hampir sebagian besar masyarakat setuju bahwa *internet* merupakan sebuah kemajuan yang banyak memberikan manfaat, terutama dari aspek kebutuhan akan barang dan jasa. Berkembangnya internet juga turut membantu pelaku bisnis untuk terus berinovasi menciptakan sebuah model bisnis baru yang dapat menjadi penyedia perkembangan kebutuhan masyarakat. Salah satu penyedia layanan transportasi berbasis *internet* adalah *Go-Jek*.

Go-Jek merupakan aplikasi *mobile* untuk layanan transportasi berbasis lokasi. Sehingga konsumen dapat melakukan order yang diterima oleh pengemudi ojek terdekat. Sehingga konsumen dapat memantau langsung lokasi pengemudi ojek yang akan mengantarnya. *Go-Jek* yang didirikan oleh Nadiem Makarim dan Michaelangelo Moran pada awal kemunculannya pada tahun 2010 (Wulandari, Syah, & Abdillah, 2016) menuai bermacam-macam respon dari masyarakat. Namun seiring berjalannya waktu dan berkembangnya pemahaman masyarakat, *Go-Jek* dapat diterima dan

berkembang pesat di industri transportasi Indonesia. *Go-Jek* kemudian melakukan banyak inovasi dalam layanannya, seperti *Go-Massage*, *Go-Food*, *Go-Clean*, *Go-Tix*, dan lain-lain yang banyak diminati konsumennya. Beberapa saat setelah kemunculannya, *Go-Jek* menyertakan fitur *Go-Jek Credit* yang merupakan dompet *virtual* guna mempermudah transaksi secara *online*.

Go-Jek Credit adalah sebuah sistem pembayaran online yang disediakan oleh *Go-Jek* bagi konsumen yang tidak menghendaki pembayaran secara tunai. Hal ini tentu saja sudah tidak asing lagi untuk bisnis *E-Commerce* di Indonesia, karena *Go-Jek Credit* bisa dikategorikan sebagai *M-Payment*. Sistem pembayaran seperti ini juga sudah kita temui di Indonesia seperti Mandiri e-Money, BCA Flash, dan Telkomsel T-Cash. *M-Payment* sendiri bisa diartikan sebagai salah satu jenis dari aktivitas bisnis yang melibatkan perangkat elektronik yang memiliki koneksi dengan *mobile network* agar dapat berjalan (Liébana-Cabanillas, Sánchez-Fernández, & Muñoz-Leiva, 2014). Fitur *Go-Jek Credit* awalnya belum banyak digunakan oleh pengguna *Go-Jek* karena mereka hanya memerlukan layanan ojek. Namun, seiring berjalannya waktu dan semakin luas inovasi layanan yang ditawarkan oleh *Go-Jek*, fitur ini menjadi banyak digunakan oleh konsumen *Go-Jek* dan saat ini namanya berubah menjadi *Go-pay*.

Go-pay merupakan salah satu produk *Financial Technology* yang diusung oleh *Go-Jek* untuk mempermudah sistem keuangan dalam perusahaan. Faktor internal berupa heterogenitas perusahaan dan tingkat persaingan serta faktor eksternal berupa peraturan pemerintah dan standart teknologi turut membentuk terjadinya inovasi pembayaran dari metode konvensional menjadi *mobile payment* (Liu, Kauffman, & Ma, 2015).

Terlepas dari berkembangnya sebuah inovasi dalam proses bisnis, perusahaan terlebih dulu harus mengenal konsumennya, hal tersebut diperlukan dalam rangka mengkaji kebutuhan para konsumen. Pemahaman terhadap konsumen akan turut serta menentukan pencapaian kinerja yang maksimal dari perusahaan dalam melakukan pengembangan terhadap produk yang diberikan kepada konsumen (Nelwan, 2015).

Walaupun *Go-Jek* telah melengkapi sistem pembayarannya dengan produk dompet virtual *Go-pay*, tidak sedikit pengguna gojek yang masih memilih metode pembayaran tunai dengan berbagai alasan. Hal ini menimbulkan pertanyaan yang mendasar tentang kemunculan *Go-pay*. Apakah kehadiran *Go-pay* dalam *Go-jek* dapat diterima oleh konsumen sebagai sebuah kemajuan teknologi yang harus ada dalam era

modern ini, dan apakah adanya fitur *Go-pay* mempengaruhi intensitas penggunaan *Go-Jek*.

Dilansir flip.id (2021), di era yang serba digital semua sistem transaksi juga dialihkan secara digital. Bukan hanya lewat internet banking saja, tetapi telah hadir aplikasi populer untuk transaksi yang disebut sebagai dompet digital. Aplikasi ini berkembang begitu pesat di Indonesia, hingga muncul beberapa platform dengan berbagai keunggulannya masing-masing. Dompet digital atau dikenal juga sebagai *e wallet* semakin populer untuk digunakan karena berbagai kelebihan yang dimiliki. Tidak heran bahwa semakin banyak yang beralih menggunakan sistem transaksi ini. Ada banyak jenis *e-wallet* terbaik di Indonesia yang semakin hari semakin diminati oleh banyak pengguna. Ada 7 aplikasi *e-wallet* yang sering digunakan antara lain : 1. Aplikasi DANA, 2. Aplikasi OVO, 3. Aplikasi *Go-Pay*, 4. Aplikasi DOKU, 5. Sakuku, 6. Aplikasi LinkAja, 7. Aplikasi Jenius.

Dilansir oleh nasional tempo (2021), masyarakat belakangan dihebohkan dengan dugaan kebocoran sebanyak 1,3 juta data pribadi pengguna electronic Health Alert Card (eHAC). Persoalan tersebut menjadi perhatian banyak orang karena aplikasi tersebut selama ini digunakan untuk kepentingan pelacakan COVID-19 dalam pemenuhan persyaratan penerbangan. Temuan kebocoran data pengguna eHAC pertama kali ditemukan oleh peneliti vpnMentor. Dilansir dari vpnmentor.com, 1,3 juta data pengguna eHAC pertama kali ditemukan di sebuah server yang bisa diakses oleh semua orang. Temuan tersebut membuat data pengguna eHAC menjadi sangat rentan untuk disalahgunakan. Adapun beberapa data yang bocor, antara lain nama, alamat rumah, nomor ID, rumah sakit tempat melakukan tes COVID-19, dan sebagainya. Ada 6 kasus kebocoran data di Indonesia, antara lain : 1. Kebocoran data BPJS Kesehatan, 2. Kebocoran data Lazada, 3. Kebocoran data Cermati, 4. Penjualan data nasabah BRI Life, 5. Kebocoran data Tokopedia, 6. Kebocoran data Komisi Pemilihan Umum.

Menurut Al-Sehri (2012), salah satu faktor yang menjadi pemicu terjadinya pelanggaran keamanan informasi dan privasi adalah karena pengguna *smartphone* memiliki kesadaran yang tidak memadai dalam menggunakan *smartphone* dengan aman, beberapa dari mereka memiliki pengetahuan yang cukup memadai dalam penggunaan *smartphone* tetapi mereka tidak menerapkannya dengan baik.

Menurut Xu et al. (2012), praktik agresif seperti akses data yang digunakan oleh pengembang aplikasi mobile dan sistem operasi telah memperburuk masalah privasi di antara pengguna (*smartphone*). Kekhawatiran ini terkait dengan 'koleksi otomatis' dari pengguna perangkat mobile, informasi keberadaan secara real-time, dan kerahasiaan data yang dikumpulkan seperti lokasi, identitas pribadi, dan perilaku sehari-hari. Berbeda dengan internet konvensional, *platform mobile* memungkinkan untuk *real-time* dan komunikasi data dan transmisi yang selalu menyala, yang menimbulkan ancaman privasi. Informasi Privasi menjadi kekhawatiran pengguna tentang kemungkinan kehilangan privasi sebagai akibat dari pengungkapan informasi kepada pihak ketiga seperti pengembang aplikasi. Teori ini memaparkan bahwa *smartphone* yang sangat dikenal khususnya Android merupakan sistem operasi mobile phone yang memiliki resiko yang besar, masih banyak pengguna *smartphone* yang belum menyadari aturan keamanan dan privasi yang harus diperhatikan dalam menggunakan *smartphone*. Padahal, banyak kasus-kasus terjadi seputar dampak negatif karena kurangnya kesadaran keamanan dan privasi dalam menggunakan *smartphone*, termasuk di Indonesia, diakibatkan oleh faktor ketidakpahaman akan keamanan informasi dan privasi ketika mendapatkan *SMS/email* dari orang tidak dikenal yang menyertakan link palsu yang merupakan website buatan penyerang untuk membuat *smartphone* terkena serangan *malware* yang mengakibatkan pengambilan data secara illegal sampai rusaknya internal dari perangkat (*smartphone*) yang digunakan.

LANDASAN TEORI

Privasi

Informasi privasi mengacu pada individu, kelompok, atau institusi untuk menentukan diri mereka sendiri dan bagaimana tentang luasnya informasi tentang apa yang dikomunikasikan pada orang lain (Malhotra et al, 2004). Menurut Smith et al. (2011), terdapat empat definisi privasi informasi yaitu privasi sebagai hak asasi manusia, privasi sebagai komoditas, privasi sebagai keadaan akses terbatas, dan privasi sebagai kemampuan untuk mengendalikan informasi tentang diri sendiri.

Perhatian informasi privasi mengacu pada suatu padangan hubungan individu dalam konteks informasi privasi. Privasi dipengaruhi oleh kondisi eksternal seperti industri, budaya, dan hukum. Bagaimana pun, suatu persepsi individu kondisi eksternal

juga berbeda menurut karakteristik pribadi dan pengalaman masa lalu. Oleh karena itu orang sering berbeda pendapat mengenai toko *online* dan penggunaan informasi pribadi mereka.

Pertumbuhan teknologi baru untuk mengolah kompleksitas informasi. Sebagai konsekuensi kecurigaan konsumen terus meningkat mengenai data pribadi mereka. Privasi secara instrument bernilai sebab diperlukan pengembangan hubungan kepercayaan dan kedekatan pada waktu yang sama (Anil Gurung, 2006). Privasi diuji atas dasar kebenaran informasi.

Menurut Xu et al. (2012), persepsi pengguna smartphone dari sudut pandang pengawasan terhadap pengguna bisa sangat menonjol karena kegiatan pengumpulan data yang agresif oleh aplikasi mobile. Kedua, persepsi intrusi dapat dipicu ketika aturan kepemilikan dilanggar, yaitu, ketika aplikasi mobile mampu membuat keputusan independen tentang memiliki atau meminta informasi pribadi pengguna. Dalam penelitian ini dan berdasarkan penelitian sebelumnya privasi terdiri dari tiga indikator yaitu *perceived surveillance*, *perceived intrusion*, *secondary use information* (Xu et al., 2012).

Keamanan

Kejahatan dalam media *internet* berjumlah sangat besar serta memiliki bentuk yang beragam karena beberapa alasan. Pertama, identitas individu atau organisasi dalam dunia *internet* mudah untuk dipalsukan, tetapi sulit dibuktikan secara hukum. Kedua tidak membutuhkan sumber daya ekonomi yang besar untuk melakukan kejahatan dalam *internet*. Ketiga *internet* menyediakan akses yang luas pada pengguna yang potensial menjadi korban. Keempat kejahatan dalam *internet*, identitas pelaku tidak dikenal dan secara yuridis sulit mengejar pelaku. Rasa aman mungkin menggambarkan subyektif sebagai kemungkinan konsumen percaya bahwa informasi pribadi mereka (*Private* dan *moneter*) akan tidak dapat dilihat, dan berpindah tanpa persetujuan.

Menurut Whitman dan Mattord (2011), keamanan informasi merupakan upaya untuk melindungi informasi dan elemen-elemen penting yang ada didalamnya, baik berupa sistem atau perangkat keras yang digunakan untuk menyimpan dan mengirimkan informasi. Menurut McLeod dan Schell (2008) keamanan informasi ditujukan untuk mencapai tiga tujuan utama, yaitu kerahasiaan ketersediaan, dan integritas.

Dalam transaksi *online* bahwa keamanan sistem informasi berbasis *internet* menjadi suatu keharusan untuk diperhatikan, Karena jaringan komputer *internet* bersifat publik dan global pada dasarnya tidak aman. Pada saat data terkirim dari suatu komputer ke komputer lain di dalam *internet*, data ini akan melewati sejumlah komputer lain yang bisa memberi kesempatan kepada pengguna *internet* lain untuk menyadap atau mengubah data tersebut. Pembobolan sistem keamanan di *internet* hampir setiap hari terjadi di seluruh dunia. Resiko bertransaksi melalui *internet* sangat dimungkinkan, penyusup berhasil mengakses komputer dalam jaringan yang dilindungi. Jika terjadi ketidaknyamanan dalam jaringan komputer menjadi beban bagi pelaku usaha dalam hal tanggung jawabnya.

Kegiatan dalam *e-commerce* disamping memberikan keuntungan dalam bertransaksi secara *online*, disisi lain mengandung beberapa resiko diantaranya adalah, gangguan *website* yang diakibatkan oleh para *hacker*. *Hacker* memungkinkan untuk masuk, mengacak-acak dan sekaligus menjarah apa yang dirasakan menguntungkan mereka. Para *hacker* juga dapat membuat kerusakan yang tidak dapat diperbaiki lagi, mencuri program dan data, memodifikasi atau menghapus semua data yang berharga, mengubah tampilan dan isi situs, atau mengubah situs keseluruhan.

Aktivitas para *hacker* ini sebenarnya tidak jauh berbeda dengan pencuri yang mengacak-acak dan mengambil barang milik kita. Dalam hal ini sangat penting diperlukan sistem keamanan yang mampu melindungi *website* dari gangguan para *hacker*. Masalah keamanan menjadi masalah yang cukup menentukan bagi para pengusaha *e-commerce*. Beberapa hal ini yang perlu dipertimbangkan dalam menciptakan sistem keamanan dari gangguan pelaku kejahatan yang ingin mengacaukan *website* adalah:

1. Membuat sistem cadangan yang selalu diaktifkan.
2. Melakukan backup data pribadi, atau dana kartu kredit.
3. Menggunakan peranti lunak pendeteksi virus.
4. Menggunakan peranti lunak pendeteksi penerobosan.
5. Menggunakan *firewall*.
6. Cek URL situs.
7. Ciri *internet banking*.
8. Jangan meninggalkan komputer saat mengakses transaksi *online*.

9. Hapus *temporary internet files*.
10. Mengganti *password* secara berkala.
11. Akses dari situs utama.
12. Jangan sembarang menerima *e-mail*.
13. Cek domain.
14. Biasakan untuk *logout*.

Keamanan informasi dibagi menjadi 7 indikator 5 diantaranya *trust in application repository, misconception about app testing, security and agreement message, pirated applicaion*, dan *adoption of security control* (Mylonas, 2013) ditambah 2 indikator seperti *spam sms* dan *report of security incidents* (Sari et al., 2014).

M-Payment

Mobile Payment atau yang lebih umum disebut *M-Payment* adalah sebuah bentuk pembayaran yang dilakukan dengan sebuah perangkat *mobile* yang digunakan untuk memulai, memberi kuasa dan menyetujui sebuah pertukaran suatu nilai uang untuk memperoleh suatu barang ataupun layanan jasa (Karnouskos, 2004). Selain deifinisi tersebut terdapat definisi lain yang mencoba menjelaskan secara konseptual tentang arti dari *mobile Payment* adalah sebuah bentuk baru dari proses pertukaran nilai yang hampir mirip dengan instrumen pembayaran yang lain yang juga bisa digunakan oleh konsumen, hanya saja cenderung lebih bergantung pada kecanggihan fitur dari telepon pintar dan otorisasi keuangan konsumen.(Liu et al., 2015).

Terdapat beberapa model penelitian telah dikembangkan untuk mengetahui tingkat penerimaan sebuah teknologi baru di masyarakat. Salah satunya adalah dengan model TAM (*Technology Acceptance Model*) yang sudah sangat umum digunakan untuk mengukur perilaku penerimaan terhadap suatu teknologi baru. TAM (*Technology Acceptance Model*) adalah pengembangan dari TRA (*Theory Reasoned Action*) yang sebenarnya fokus kajiannya adalah perilaku psikologis seseorang terhadap suatu objek (Davis, Bagozzi, & Warshaw, 1989). Model klasik TAM menggunakan faktor sikap pada beberapa variabel antara lain;

1. Kemudahan dalam Penggunaan (*Ease of Use*)
2. Kemanfaatan (*Usefulness*).

M-Payment Go-Pay merupakan media transaksi pembayaran non-tunai yang memberikan kemudahan dan kenyamanan dalam melakukan transaksi pembayaran pada aplikasi *Go-Jek*. Aplikasi *Go-Jek* merupakan aplikasi canggih yang menyediakan berbagai layanan yang cukup lengkap, mulai dari transportasi, logistik, pembayaran, layanan antar makanan, dan berbagai layanan on-demand lainnya yang diciptakan oleh Nadiem Makarim dan Michaelangelo Moran pada tahun 2010. Layanan Pembayaran *Go-Pay* dilengkapi 4 fitur dan produk, yaitu *Go-Bills*, *Go-Pulsa*, *Transfer Go-Pay*, Tarik tunai *Go-Pay*, dan *Top-up Saldo Go-Pay*.

METODE PENELITIAN

Metode penelitian yang digunakan adalah metode kuantitatif jenis penelitian yang digunakan dalam penelitian ini adalah deskriptif kuantitatif. Dalam penelitian ini yang dijadikan populasi adalah mahasiswa Universitas Pamulang tingkat 1, yang berjumlah 974 orang. Pada penelitian ini sampel yang digunakan sebanyak 91 orang. Dalam penelitian ini menggunakan teknik *probability sampling* yaitu sampel acak sederhana (*simple random sampling*).

HASIL PENELITIAN

Pengaruh Privasi (X₁) Terhadap *Mobile Payment* (Y)

Berdasarkan hasil penelitian menunjukkan bahwa, terdapat pengaruh positif dan signifikan antara Privasi (X₁) Terhadap *Mobile Payment* (Y). Hal ini dibuktikan dengan persamaan regresi linear sederhana $Y = a + b(x)$ adalah $Y = 23,745 + 0,526(X_1)$. Konstanta $a = 23,745$ menunjukkan bahwa, nilai *Mobile Payment* (Y) saat ini diasumsikan bernilai 23,745 satuan dengan asumsi variabel Privasi (X₁) bernilai tetap. Konstanta $b = 0,526$ menunjukkan bahwa, jika terdapat kenaikan satu-satuan pada variabel Privasi (X₁) maka nilai *Mobile Payment* (Y) akan bertambah sebesar 0,526 satuan. Uji hipotesis menunjukkan bahwa nilai t_{hitung} variabel Privasi (X₁) terhadap *Mobile Payment* (Y) sebesar $t_{hitung} 3,860 > t_{tabel} 1,98698$ atau nilai $Sig 0,000 < 0,05$ maka H_{01} di tolak dan artinya terdapat pengaruh positif dan signifikan antara Privasi (X₁) terhadap *Mobile Payment* (Y). Nilai korelasi $R = 0,379$ berada pada rentang 0,200 – 0,399 dengan tingkat hubungan rendah, artinya Privasi (X₁) memiliki tingkat hubungan rendah terhadap *Mobile Payment* (Y). Nilai $R Square = 0,143$ dapat

disimpulkan bahwa, Privasi (X_1) memberikan kontribusi terhadap *Mobile Payment* (Y) sebesar 14,3% dan sisanya 85,7% dipengaruhi oleh faktor lain.

Hasil penelitian ini sejalan dengan hasil penelitian terdahulu yang telah dilakukan dan diteliti oleh Gatot Efrianto dan Nia Tresnawaty (2020) dengan judul kepercayaan dan pengalaman terhadap penggunaan fintech di kalangan masyarakat kabupaten tangerang Banten dengan hasil pengaruh privasi, keamanan, kepercayaan dan pengalaman secara simultan berpengaruh positif dan signifikan terhadap penggunaan fintech di kalangan masyarakat Kabupaten Tangerang.

Pengaruh Keamanan (X_2) Terhadap *Mobile Payment* (Y)

Berdasarkan hasil penelitian menunjukkan bahwa, terdapat pengaruh positif dan signifikan antara Keamanan (X_2) Terhadap *Mobile Payment* (Y). Hal ini dibuktikan dengan persamaan regresi linear sederhana $Y = a + b(x)$ adalah $Y = 5,195 + 0,878(X_2)$. Konstanta $a = 5,195$ menunjukkan bahwa, nilai *Mobile Payment* (Y) saat ini diasumsikan bernilai 5,195 satuan dengan asumsi variabel Keamanan (X_2) bernilai tetap. Konstanta $b = 0,878$ menunjukkan bahwa, jika terdapat kenaikan satu-satuan pada variabel Keamanan (X_2) maka nilai *Mobile Payment* (Y) akan bertambah sebesar 0,878 satuan. Uji hipotesis menunjukkan nilai t_{hitung} variabel Keamanan (X_2) terhadap *Mobile Payment* (Y) sebesar $t_{hitung} 8,667 > t_{tabel} 1,98698$ atau nilai $Sig 0,000 < 0,05$ maka H_{o2} di tolak dan artinya terdapat pengaruh positif dan signifikan antara Keamanan (X_2) terhadap *Mobile Payment* (Y). Nilai korelasi $R = 0,677$ berada pada rentang 0,600 – 0,799 dengan tingkat hubungan tinggi, artinya Keamanan (X_2) memiliki tingkat hubungan tinggi terhadap Kinerja *Mobile Payment* (Y). Nilai $R Square = 0,458$ dapat disimpulkan bahwa, Keamanan (X_2) memberikan kontribusi terhadap *Mobile Payment* (Y) sebesar 45,8% dan sisanya 54,2% dipengaruhi oleh faktor lain.

Hasil penelitian ini sejalan dengan hasil penelitian terdahulu yang telah dilakukan dan diteliti oleh Sally Lau, Mochammad Nugraha Reza Pradana (2021) yang berjudul pengaruh keamanan, kecepatan transaksi dan kenyamanan terhadap penggunaan mobile payment dan hasilnya keamanan berpengaruh signifikan terhadap penggunaan *mobile payment*, yang artinya keamanan merupakan hal yang sangat di butuhkan pelanggan dalam penggunaan aplikasi *mobile payment*.

Pengaruh Privasi (X_1), dan Keamanan (X_2) Terhadap *Mobile Payment* (Y)

Berdasarkan hasil penelitian menunjukkan bahwa, terdapat pengaruh positif dan signifikan secara simultan antara Privasi (X_1) dan Keamanan (X_2) Terhadap *Mobile Payment* (Y). Persamaan regresi linear berganda $Y = a + b_1X_1 + b_2X_2$ adalah $Y = 1,516 + 0,183(X_1) + 0,810(X_2)$, Konstanta $a = 1,516$ menunjukkan bahwa, nilai *Mobile Payment* (Y) saat ini diasumsikan bernilai 1,516 satuan dengan asumsi variabel Privasi (X_1) dan Keamanan (X_2) bernilai tetap. Konstanta $b_1X_1 = 0,183$ menunjukkan bahwa, jika terdapat kenaikan satu-satuan pada variabel Privasi (X_1) maka nilai *Mobile Payment* (Y) akan bertambah sebesar 0,183 satuan. Konstanta $b_2X_2 = 0,810$ menunjukkan bahwa, jika terdapat kenaikan satu-satuan pada variabel Keamanan (X_2) maka nilai *Mobile Payment* (Y) akan bertambah sebesar 0,810 satuan. Uji hipotesis menunjukkan bahwa nilai $F_{hitung} 39,374 > F_{tabel} 3,10$ atau probabilitas $Sig 0,000 < 0,05$ maka H_0 di tolak dan H_a di terima artinya signifikan dengan demikian hipotesis yang diajukan menetapkan terdapat pengaruh positif dan signifikan secara bersama-sama antara Privasi (X_1) dan Keamanan (X_2) Terhadap Penggunaan *Mobile Payment* (Y). Nilai korelasi $R = 0,687$ berada pada rentang $0,600 - 0,799$ dengan tingkat hubungan kuat, artinya Privasi (X_1) dan Keamanan (X_2) memiliki tingkat hubungan kuat terhadap *Mobile Payment* (Y). Nilai $R Square = 0,472$ dapat disimpulkan bahwa, Privasi (X_1) dan Keamanan (X_2), Terhadap *Mobile Payment* (Y) memberikan kontribusi sebesar 47,2% dan sisanya 52,8% dipengaruhi oleh faktor lain.

KESIMPULAN

Berdasarkan hasil penelitian menunjukkan bahwa :

1. Terdapat pengaruh positif dan signifikan antara Privasi (X_1) terhadap *Mobile Payment* (Y).
2. Terdapat pengaruh positif dan signifikan antara Keamanan (X_2) terhadap *Mobile Payment* (Y).
3. Berdasarkan hasil penelitian menunjukkan bahwa, terdapat pengaruh positif dan signifikan antara Privasi (X_1) dan Keamanan (X_2) terhadap *Mobile Payment* (Y).

DAFTAR PUSTAKA

Al-Sehri, 2012. Information security awareness and culture, *British Journal of Arts and Social Sciences*; 6(1): 61-69.

- Anil Gurung 2006 “Empirical Investigation of the Relationship of Privacy Security, and Trust with Behavioral Intention to transact in E-Commerce” The University of Texas at Arlington.
- Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Management Science*, 35(8), 982–1003. <https://doi.org/10.1287/mnsc.35.8.982>
- Flip.id. 2021. Aplikasi Dompot Digital Terbaik. <https://flip.id/blog/aplikasi-dompot-digital-terbaik>. Diakses tanggal 11 Mei 2022
- Gatot Efrianto, N. T. (2021). PENGARUH PRIVASI, KEAMANAN, KEPERCAYAAN DAN PENGALAMAN TERHADAP PENGGUNAAN FINTECH DI KALANGAN MASYARAKAT KABUPATEN TANGERANG BANTEN. *Jurnal Ilmiah Akuntansi dan Ekonomi* Volume. 1 Nomor. 6, 53-72.
- Karnouskos, S. (2004). Mobile payment: A journey through existing procedures and standardization initiatives. *IEEE Communications Surveys & Tutorials*, 6(4), 44–66. <https://doi.org/10.1109/COMST.2004.5342298>
- Kominfo. 2014. Pengguna Internet Indonesia Nomor Enam Dunia. https://kominfo.go.id/content/detail/4286/pengguna-internet-indonesia-nomor-enam-dunia/0/sorotan_media. Diakses tanggal 11 Mei 2022
- Liébana-cabanillas, F., Sánchez-fernández, J., & Mu, F. (2014). International Journal of Information Management The moderating effect of experience in the adoption of mobile payment tools in Virtual Social Networks?: The m-Payment Acceptance Model in Virtual Social Networks (MPAM-VSN), 34, 151–166. <https://doi.org/10.1016/j.ijinfomgt.2013.12.006>
- Liu, J., Kauffman, R. J., & Ma, D. (2015). Competition, cooperation, and regulation: Understanding the evolution of the mobile payments technology ecosystem. *Electronic Commerce Research and Applications*, 14(5), 372–391. <https://doi.org/10.1016/j.elerap.2015.03.003>
- McLeod, Raymond & Schell, George P. 2008. *Sistem Informasi Manajemen*, Edisi 10. Jakarta: Salemba Empat.
- Mylonas, A., Kastania, A., Gritzalis, D., 2013. Delegate the smartphone user? Security awareness in smartphone platforms. *Computer & Security* Volume 34 : 47-66.
- Nasional Tempo. 2021. 6 Kasus Kebocoran Data Pribadi Di Indonesia. <https://nasional.tempo.co/read/1501790/6-kasus-kebocoran-data-pribadi-di-indonesia>. Diakses tanggal 11 Mei 2022
- Nelwan, E. F. (2015). Analisis Faktor Faktor, (Nelwan) 25, 25–43. IDCERT, 2015. Laporan Dwi Bulan I 2015. Indonesia Computer Emergency Response.
- Sally Lau, M. N. (2021). Pengaruh Keamanan, Kecepatan Transaksi dan Kenyamanan Terhadap Penggunaan Mobile Payment. *KINERJA* 18 (2), 288-295.
- Sari, Kencana, P., Candiwan, 2014. Measuring Information Security Awareness of Indonesian Smartphone Users. *TELKOMNIKA*. Vol.12, No.2, June 2014, pp.493-500.

- Smith, H.J., Dinev, T., Xu, H., 2011. Information Privacy Research: An Interdisciplinary Review, *MIS Quarterly* (35:4), pp 989-1015.
- Witman, M. E., Mattord, H. J., 2011. *Principles of Information security*, 4th Edition. Atlanta: Cengage Learning.
- Wulandari, C., Syah, L. Y., & Abdillah, L. A. (2016). Analisa Tingkat Kepuasan Layanan TI (Studi Kasus Pada Aplikasi Gojek). *Teknologi Informasi Dan Komunikasi Ke-8 (SEMNASTIK2016)*, 8, 7–12.
- Xu, H., Gupta, S., Rosson, M.B., Carroll, J.M., 2012. Measuring Mobile Users' Concerns for Information Privacy. *Thirty Third International Conference on Information Systems*, Orlando.