EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647
Website: https://journal.fkpt.org/index.php/Explorer DOI: https://doi.org/10.47065/explorer.v5i1.1817

Metode One Time Pad sebagai Verifikasi Akun E-Wallet dalam Pencegahan Cybercrime

Sarifah[1*], Ilham Faisal[2], Imran Lubis[3]
[1,2,3] Program Studi Teknik Informatika, Fakultas Teknik dan Komputer, Universitas Harapan Medan, Indonesia
[1*]syarifah.rifarifa@gmail.com, [2]ilhamfaisal@unhar.ac.id, [3]imranlubis@unhar.ac.id
[*)] syarifah.rifarifa@gmail.com

Abstrak−Penelitian ini bertujuan untuk meningkatkan keamanan pada saat dimana setiap kali pengguna melakukan login atau transaksi, sebuah OTP (*One time pad*) akan dikirim melalui email, kode OTP dihasilkan secara acak hanya dapat diakses oleh pihak akun yang memiliki kunci OTP yang sah dan valid pada waktu tertentu. Dengan menggunakan algoritma *one time pad* memberikan tingkat keamanan yang sangat tinggi, karena OTP yang dihasilkan bersifat unik untuk setiap transaksi. Namun implementasinya menuntut disiplin ketat dalam pengelolaan kunci dan proses enkripsi atau dekripsi yang tepat agar dapat berfungsi secara optimal. Sistem ini dirancang untuk keamanan pengguna akun agar tidak terjadi kebocoran data, sehingga meminimalkan potensi kejahatan seperti pencurian identitas dan penipuan. Dari hasil penelitian menunjukkan bahwa tidak ada satu pun OTP yang berulang dalam 10 kali transaksi yang dilakukan. Setiap kode OTP yang dihasilkan unik dan berbeda dari OTP sebelumnya, baik pada transaksi yang berhasil maupun yang gagal, membuktikan efektivitas sistem. Website ini dibuat dengan menggunakan Visual Studio Code untuk memastikan implementasi sistem yang stabil dan efisien.

Kata Kunci: Metode One Time Pad, E-Wallet, Cybercrime,Website

Abstract−This research aims to improve security when every time a user logs in or makes a transaction, an OTP (One time pad) will be sent via email, the OTP code is generated randomly and can only be accessed by the account party that has a valid and valid OTP key at that time. certain. Using the one time pad algorithm provides a very high level of security, because the resulting OTP is unique for each transaction. However, its implementation requires strict discipline in key management and proper encryption or decryption processes so that it can function optimally. This system is designed for account user security to prevent data leaks, thereby minimizing the potential for crimes such as identity theft and fraud. The research results show that not a single OTP was repeated in the 10 transactions carried out. Each OTP code generated is unique and different from previous OTPs, both on successful and failed transactions, proving the effectiveness of the system. This website was created using Visual Studio Code to ensure a stable and efficient system implementation.

Keywords: One Time Pad Method, E-Wallet, Cybercrime, Website

1. PENDAHULUAN

E-Wallet adalah alat pembayaran non-tunai yang mempunyai tujuan untuk mempermudah masyarakat dalam melakukan pembayaran atau transaksi jual beli[1]. E-Wallet juga memiliki dua komponen utama, yaitu perangkat lunak dan informasi. Pada perangkat lunak tersebut memuat informasi pribadi dan fasilitas keamanan serta enkripsi data. Ini memberikan cara yang mudah dan aman untuk membeli (atau) menerima pembayaran perincian yang diberikan oleh pelanggan yang mencakup nama, alamat pengiriman, metode pembayaran, jumlah yang harus dibayar, rincian kartu kredit atau debit, dan lain-lain [2]. Indonesia memiliki 42 e-wallet yang terdaftar di Bank Indonesia. Namun, ada 10 E-Wallet yang memiliki pengguna terbanyak, yaitu GoPay, Ovo, Dana, Link Aja, Jenius, Go Mobile, iSaku, Sakuku, Doku, dan Paytren eMoney [3]. Aplikasi Dana dan Gopay berhasil memperoleh peringkat teratas startup digital payment yang paling banyak diketahui oleh masyarakat Indonesia dengan persentase Dana sebesar 99% dan Gopay 98% dapat disimpulkan bahwa Dana dan Gopay memiliki kelebihan dan hal-hal yang mempengaruhi pengguna aktifnya. Faktor pengguna aktif tersebut mendorong peneliti untuk melakukan penelitian dan menentukan produk layanan dompet digital terbaik antara Dana dan Gopay[4].

Mengingat banyaknya *E-Wallet* yang telah beredar ditengah masyarakat tentu akan rawan pencurian data. Untuk itu perlu sebuah metode untuk menjaga keamanan data. Peneltian ini berfokus pada cara memperkuat verifikasi akun *E-Wallet* untuk mencegah *cybercrime* melalui penerapan metode *One Time Pad*, serta kinerja metode tersebut berdasarkan tingkat keberhasilan generator dan validasi dalam memastikan keamanan data. Salah satu metode yang bisa digunakan untuk melakukan pengamanan data adalah OTP (*One Time Pad*). *Algortime One Time Pad* adalah metode yang menerapkan algoritma kunci simetris atau proses enkripsi dan dekripsi menggunakan kunci acak [5]. OTP adalah metode autentikasi yang menggunakan kode acak yang hanya dapat

EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647
Website: https://journal.fkpt.org/index.php/Explorer DOI: https://doi.org/10.47065/explorer.v5i1.1817

digunakan sekali. Sehingga kerahasiaan kunci tersebut merupakan penentuan dalam keamanan atau pesan yang dikirimkan. *One Time Pad* (OTP) memiliki beberapa kelebihan yang menjadikannya sebagai salah satu metode enkripsi paling aman. Salah satu kelebihannya yang utama adalah memberikan keamanan absolut (*perfect secrecy*), di mana pesan yang dienkripsi menggunakan OTP tidak dapat dipecahkan tanpa mengetahui kunci, bahkan dengan kekuatan komputasi modern sekalipun. Selain itu, OTP sangat tahan terhadap serangan brute force karena setiap kunci bersifat unik, acak, dan hanya digunakan satu kali, sehingga tidak ada pola yang bisa dianalisis untuk mendekripsi pesan. Keunggulan lainnya adalah OTP tidak meninggalkan jejak yang dapat dianalisis, membuatnya sangat sulit untuk dibongkar menggunakan metode analisis kriptografi [6] [7] [8] [9].

Pada suatu penelitian yang di dalamnya membahas tentang Algoritma RSA digunakan untuk pengamanan database dengan proses enkripsi dan deskripsi data sedangkan OTP digunakan untuk pengamanan proses registrasi, login serta transaksi melalui verifikasi OTP. Penelitian ini menambah algoritma RSA [10].

Penelitian lain membahas tentang implementasi algoritma enkripsi one time pad dan vigenere cipher, berbasis kriptografi merupakan salah satu metode yang digunakan untuk meningkatkan keamanan data karena dapat melakukan untuk mengamankan pesan teks. Sistem keamanan pesan tergantung seberapa sulit kunci yang digunakan, pada penelitian tersebut kunci yang digunakan algoritma One Time Pad dalam bentuk binary bukan ASCII sehingga susah ditebak dan juga kunci dihasilkan secara acak [11].

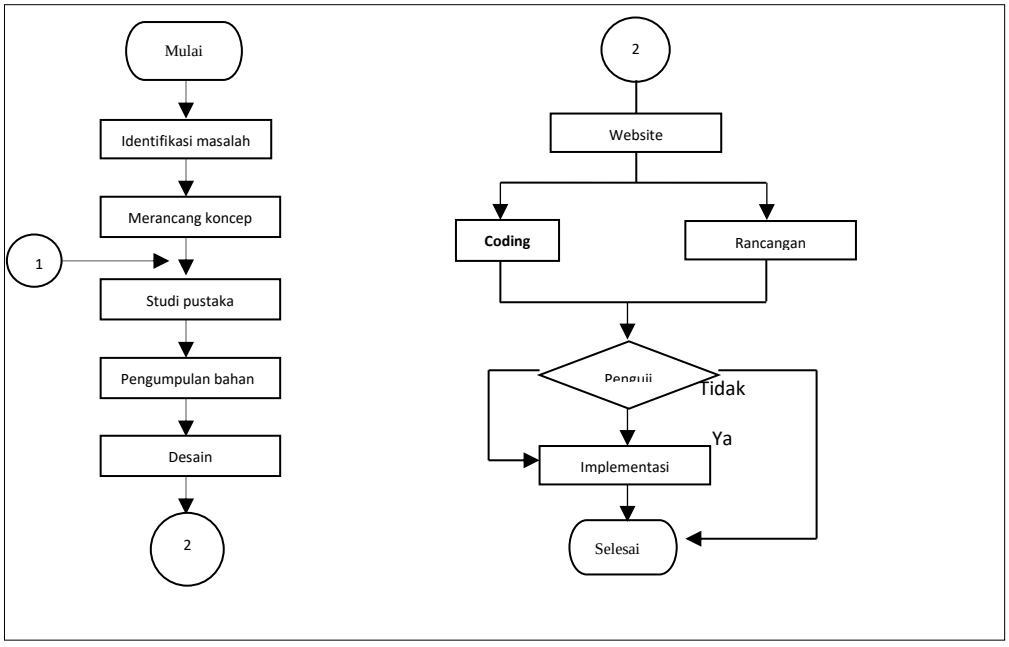
Pada penelitian lainnya membahas tentang mengamankan data pesan dengan metode one time pad chipper. Proses teknik One Time Pad Chiper dalam mengenkripsi dan dekripsikan data pesan (*file*) sehingga sulit di terjemahkan orang yang tidak berhak. Pada penelitian tersebut dengan mengubah nilai ke bentuk karakter ASCII kemudian diubah kebentuk biner setelah itu di XOR-kan dengan plainteks dengan kunci maka akan menghasilkan sebuah chiperteks yang terenkripsi. Metode One Time Pad Chiper dalam mengamankan data pesan (*file*) yaitu dengan mengenkripsi file dengan mengubah ekstensi dan nilai karakternya sehingga sulit untuk diterjemahkan oleh kriptanalisis [12].

Penelitian ini bertujuan untuk mengembangkan sistem verifikasi akun *e-wallet* berbasis website dengan menerapkan *One Time Pad* sebagai keamanan untuk meningkatkan perlindungan terhadap akses tidak sah akibat cybercrime, mempermudah pengguna dalam melakukan transaksi *online*, serta mengetahui kinerja *One Time Pad* berdasarkan tingkat keberhasilan generator dan validasi.

2. METODE PENELITIAN

2.1 Diagram Penelitian

Diagram ini menjelaskan mengenai tahapan yang dilakukan dalam penelitian seperti pada gambar 1.



Gambar 1. Diagram Penelitian

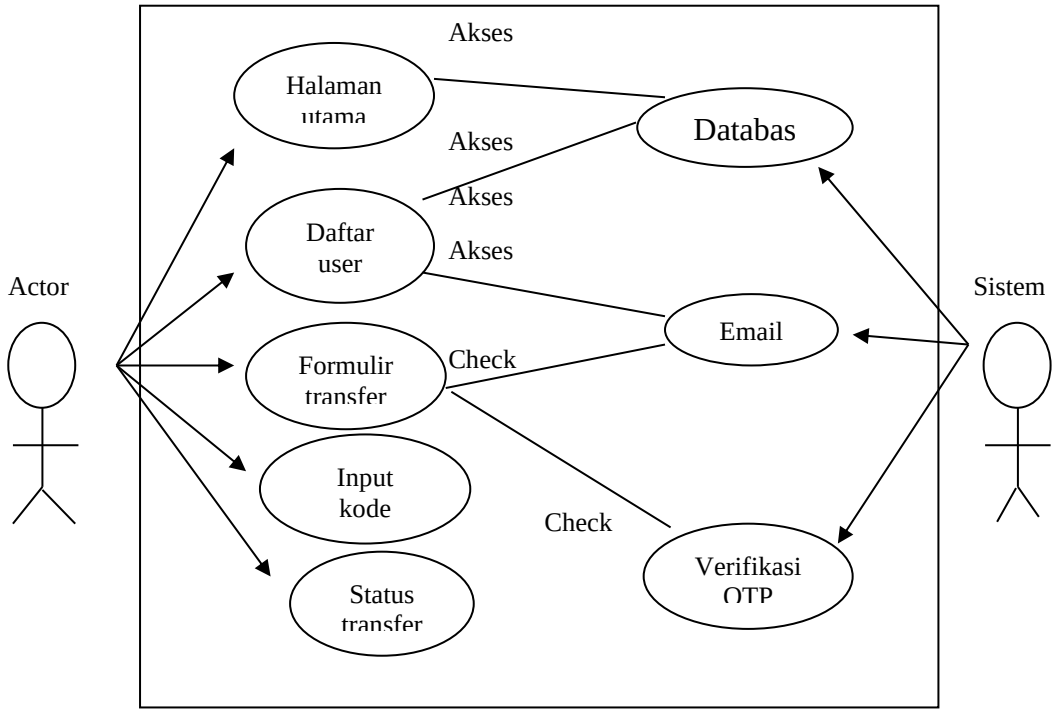
EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647
Website: https://journal.fkpt.org/index.php/Explorer DOI: https://doi.org/10.47065/explorer.v5i1.1817

2.1.1 Perancangan Website

Pada tahap ini, dibuat menggunakan diagram unified modeling language untuk memberikan proses kerja pada pembuatan *E-Wallet* berbasis *website* untuk mengamankan akun *E-Wallet*. Penjelasan UML yang digunakan seperti *use case diagram*, *sequence diagram* dan *activitiy diagram* sebagai berikut:

1. Use Case Diagram

Use case diagram digunakan untuk menggambarkan langkah-langkah dalam interaksi *website*. Terdapat actor di dalam *website* yang dirancang yaitu anggota. Dalam hal ini anggota berperan sebagai anggota *website*.

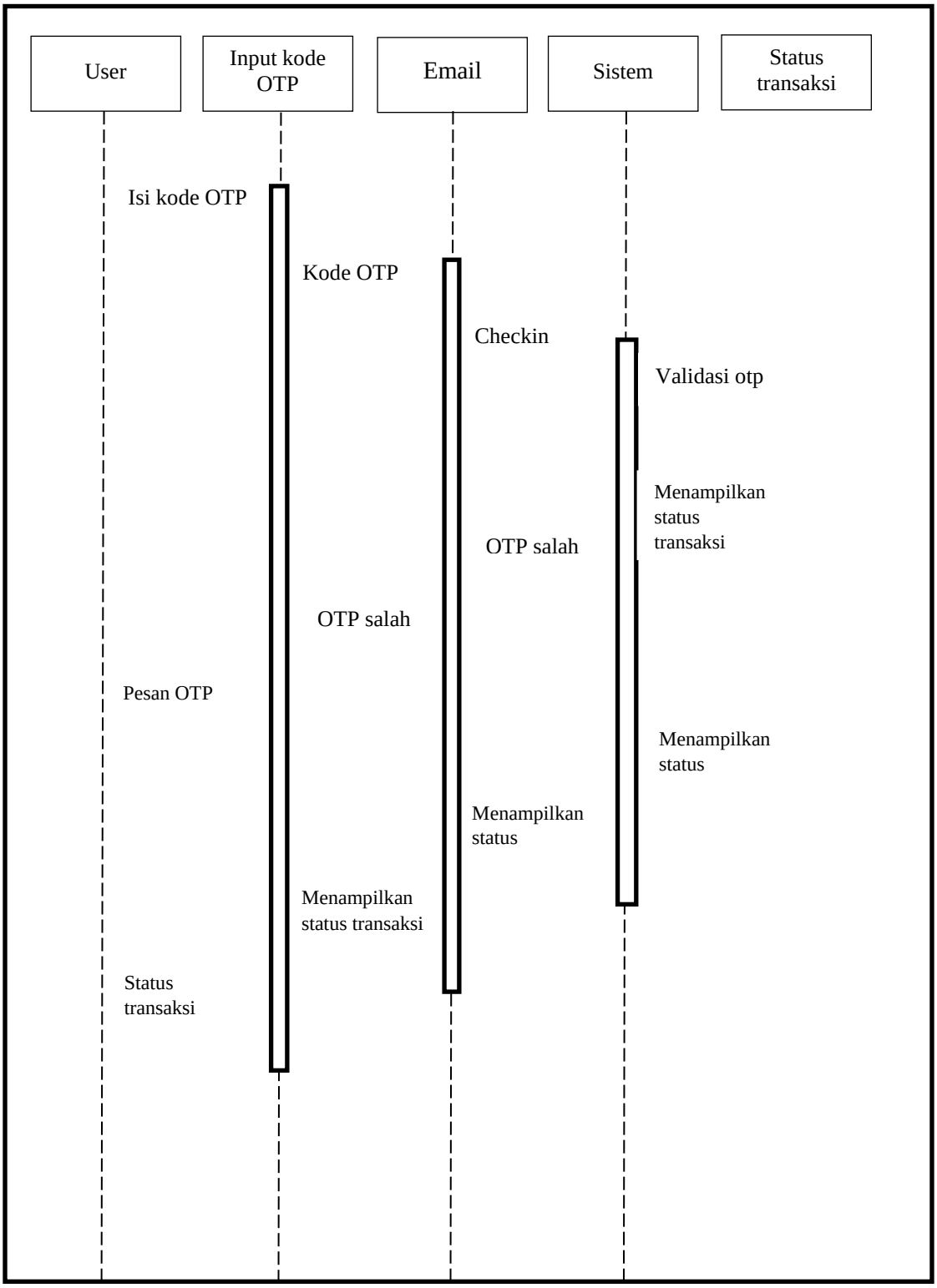


Gambar 2. *Use Case Diagram*

2. *Sequence Diagram*

Sequence diagram menggambarkan perilaku pada sebuah skenario pada *website*. *Diagram* ini menunjukkan sejumlah contoh objek dan *message* yang diletakan diantara obyek-obyek ini di dalam *use case diagram*. Biasa digunakan untuk menggambarkan skenario atau rangkaian langkah-langkah yang dilakukan sebagai respon dari sebuah *event* untuk menghasilkan *output* tertentu. *Sequence diagram* dapat dilihat pada gambar 3.

EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647
Website: https://journal.fkpt.org/index.php/Explorer
DOI: https://doi.org/10.47065/explorer.v5i1.1817



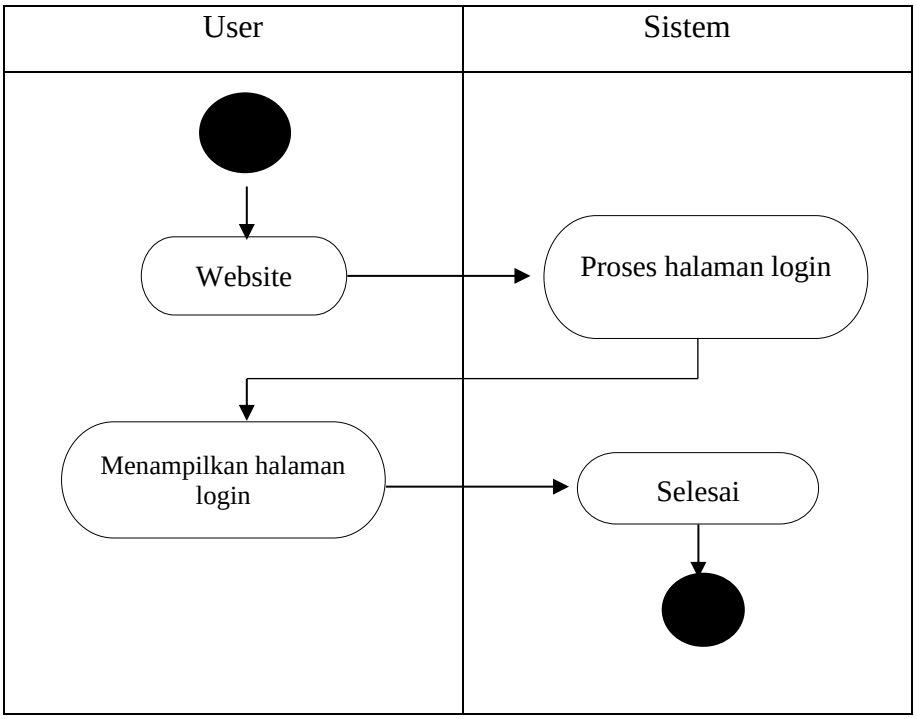
Gambar 3. *Sequence diagram input* OTP

3. *Activity Diagram*

Activity Diagram menggambarkan rangkaian aliran dari aktivitas. *Diagram* ini juga digunakan untuk memodelkan *action* yang dilakukan saat sebuah operasi dieksekusi dan memodelkan hasil dari *action* tersebut.

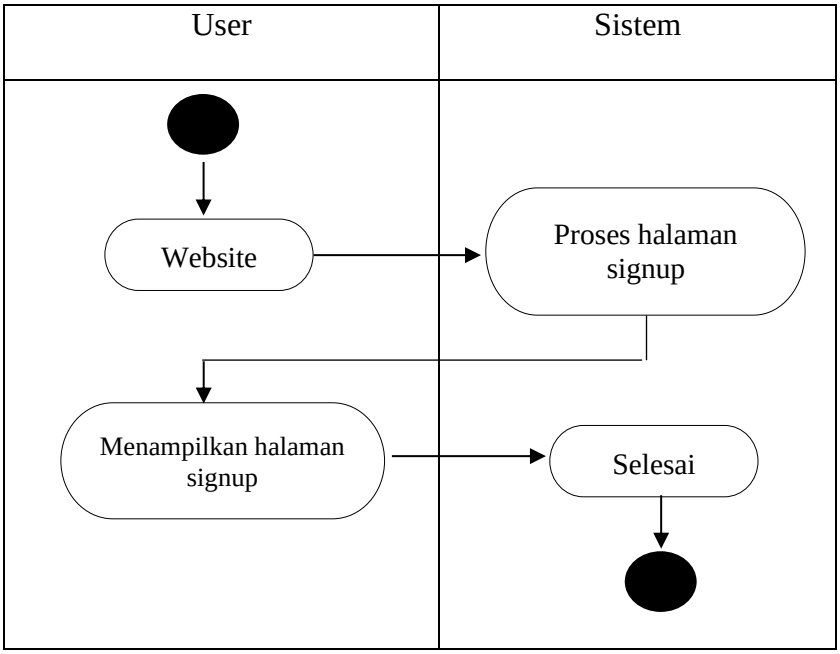
a. *Activity Diagram* halaman *login*

EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647
Website: https://journal.fkpt.org/index.php/Explorer
DOI: https://doi.org/10.47065/explorer.v5i1.1817



Gambar 4. *Activity Diagram* Halaman *Login*

b. *Activity Diagram* Halaman *Signup*

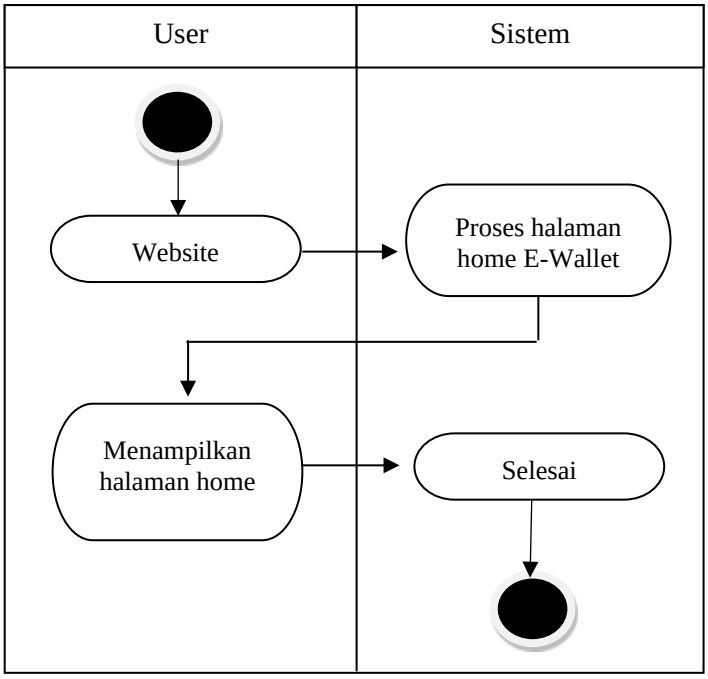


Gambar 5. *Activity Diagram* Halaman *Sigunp*

EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647
Website: https://journal.fkpt.org/index.php/Explorer DOI: https://doi.org/10.47065/explorer.v5i1.1817

c. Activity Diagram Halaman *Home*

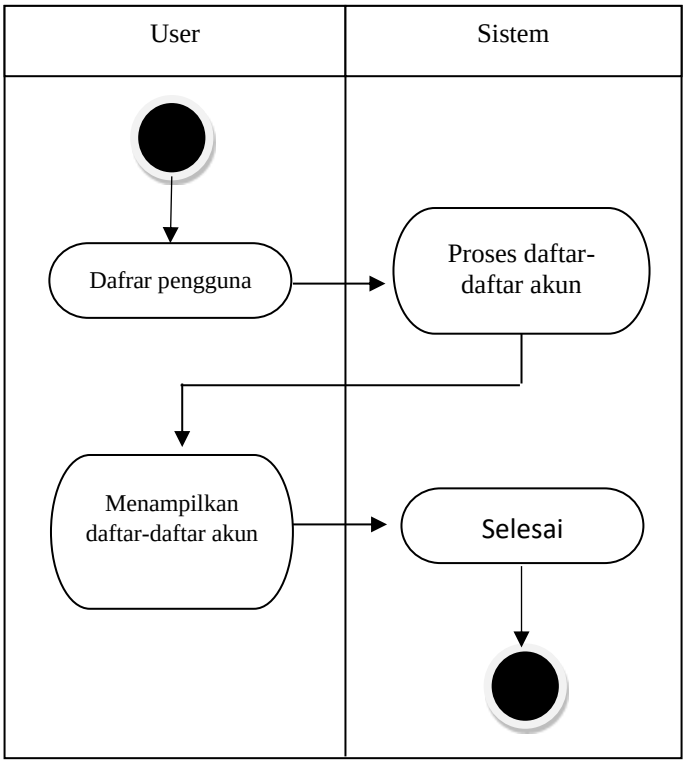
Activity Diagram ini menggambarkan logik pengguna ketika ingin mengetahui tentang informasi akun pengguna, saldo, maupun riwayat transaksi.



Gambar 6. *Activity Diagram* Halaman *Home*

d. *Activity Diagram* Daftar Akun Pengguna.

Activity Diagram Daftar Akun Pengguna akan menampilkan daftar-daftar nama akun tujuan yang akan ditransfer.

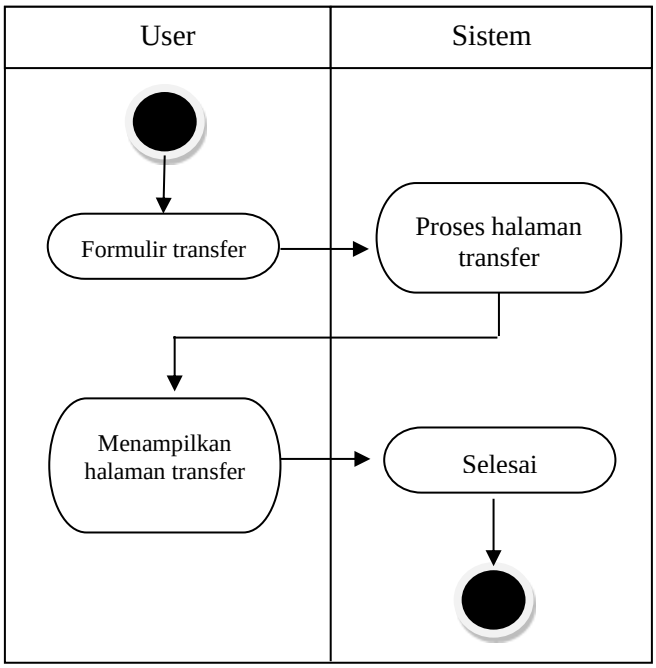


Gambar 7. *Activity Diagram* Daftar Pengguna

EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647
Website: https://journal.fkpt.org/index.php/Explorer DOI: https://doi.org/10.47065/explorer.v5i1.1817

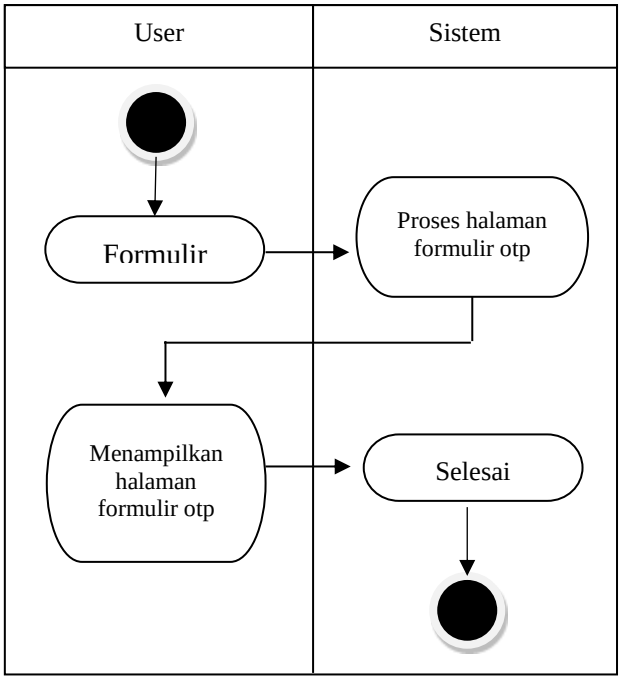
e. Activity Diagram Formulir Transfer

Activity Diagram Formulir Transfer akan menampilkan formulir transfer, memasukkan nominal uang yang akan ditransfer



Gambar 8. *Activity Diagram* Formulir Transfer

b. *Activity Diagram* Formulir OTP



Gambar 9. *Activity Diagram* Formulir OTP

2.2 Cybercrime

Cybercrime ialah suatu tindakan ilegal yang dilakukan oleh oknum pelaku kejahatan dengan menggunakan teknologi komputer dan jaringan internet untuk melakukan penyerangan sistem informasi terhadap suatu korban. Seperti halnya terjadi hack akun sosial media, membobol perangkat teknologi serta data korban, kemudian menyikat habis isi saldo di M-Banking atau kartu kartu kredit korban. Di Indonesia diatur dalam Undang-UndangNomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah

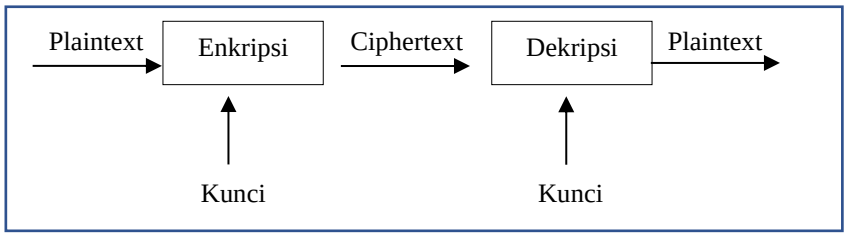
EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647
Website: https://journal.fkpt.org/index.php/Explorer DOI: https://doi.org/10.47065/explorer.v5i1.1817

menjadi UU Nomor 19 tahun 2016. *Cybercrime* termasuk dalam kategori perbuatan yang dilarang dalam UU ITE[13]. *Cybercrime* adalah tindakan criminal yang dilakukan dengan cara menggunakan teknologi komputer sebagai alat kejahatan utama. *Cybercrime* merupakan kejahatan yang memanfaatkan perkembangan teknologi komputer khususnya internet. *Cybercrime* didefinikan sebagai perbuatan melanggar hokum dan tikndakan yang dilakukan dapat mengancam dan merusak infrastruktur teknologi informasi, seperti akses illegal, percobaan atau tindakan mengakses sebagian amupun seluruh bagian sistem komputer tanpa izin dan pelaku tidak memiliki hak melakukan pengaksesan[14].

Kejahatan dunia maya adalah kejahatan yang dilakukan terhadap komputer dan sistem informasi dengan tujuan mendapatkan akses tidak sah ke suatu sistem atau mencegah pengguna yang sah untuk menggunakannya. *Cybercrime* berkembang dengan cepat, dan tren-tren baru sering bermunculan. Untuk mengatasi *Cybercrime*, penegak hukum harus selalu mengikuti perkembangan teknologi yang sedang berkembang dan memahami peluang yang ada untuk melakukan aktivitas kriminal[15].

2.2 Algoritma One Time Pad

Kriptografi adalah suatu ilmu atau seni mengamankan pesan dan dilakukan oleh *cryptographer*, sedangkan *cryptanalysis* adalah suatu ilmu dan seni membuka breaking ciphertext dan orang yang melakukannya disebut crypthanalyst[16]. Kriptografi digunakan hampir di setiap aspek kehidupan modern untuk menjaga kerahasian dan keamanan informasi dengan menggunakan persamaan matematika dalam proses enkripsi dan deskripsi[17]. Algortima OTP merupakan algoritma simetris dimana kunci yang digunakanuntuk proses enkripsi dan dekripsi merupakan kunci yang sama panjang karakter kunci dari algoritma OTP harus sesuai dengan panjang karakter dari plaintext[18]. Secara sederhana, proses algoritma one time pad dapat digambarkan seperti pada gambar 10.



Gambar 10. Proses Kriptografi

Proses enkripsi dapat dilakukan dengan persamaan matematis seperti pada persamaan 1.

$$Ci = Pi + Ki \bmod 10 \quad (1)$$

C*i* = P*i* + K*i* mod 10
C*i* = ciphertext (hasil enkripsi)
P*i* = plaintext (pesan asli)
K*i* = kunci yang digunakan untuk enkripsi

Sedangkan untuk proses deskripsi dapat dilakukan dengan persamaan 2.

$$Pi = Ci - Ki \bmod 10 \quad (2)$$

P*i* = C*i*– K*i* mod 10
P*i* = plaintext (pesan yang didekripsi)
C*i* = ciphertext (hasil enkripsi)
K*i* = kunci yang digunakan untuk dekripsi

Penerapan One Time Pad (OTP) dengan modulo 10.

a. Menentukan plaintext dan kunci
   Plaintext (p) : 1 9 2 4
   Kunci (k) : 7 8 3 5 t
b. Enkripsi dengan modulo 10
   C = (p+k) mod 10
   1) C = (1+7) mod 10
      = 8
   2) C = (p+k) mod 10
      = (9+8) mod 10
      = 7
   3) C = (p+k) mod 10
      C = (2+3) mod 10
      = 5

EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647
Website: https://journal.fkpt.org/index.php/Explorer DOI: https://doi.org/10.47065/explorer.v5i1.1817

4) C = (p+k) mod 10
= (4+5) mod 10
= 9

Chipertext = 8 7 5 9

c. Deskripsi dengan modulo 10

P = (c-k) mod 10

1) P = (8-7) mod 10
= 1

2) P = (c-k) mod 10
= (7-8) mod 10
= 9

3) P = (c-k) mod 10
= (5-3) mod 10
= 2

4) P = (c-k) mod 10
= (9-5) mod 10
= 4

Plaintext kembali menjadi 1 9 2 4. Dengan kunci yang benar, dekripsi menghasilkan plaintext asli.

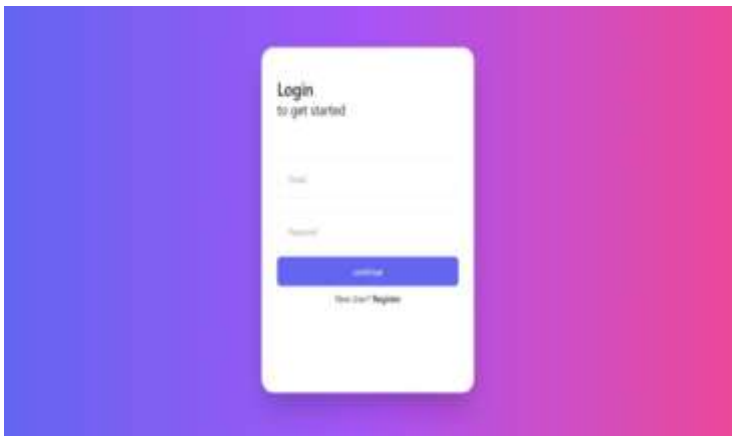
3. HASIL DAN PEMBAHASAN

3.1 Hasil

Hasil penelitian menunjukkan bahwa penerapan metode *One Time Pad* (OTP) secara signifikan dapat meningkatkan keamanan pada layanan *E-Wallet*, terutama dalam proses verifikasi akun dan perlindungan pengguna dari ancaman *cybercrime*. Algoritma OTP yang menggunakan kunci acak yang benar-benar tidak dapat diprediksi terbukti memberikan keamanan yang tinggi, karena setiap kunci hanya berlaku satu kali dan tidak dapat digunakan kembali. Proses enkripsi dilakukan dengan menambahkan angka *plaintext* dengan kunci, lalu hasilnya dimodulokan dengan 10 untuk menghasilkan *ciphertext*. Sebaliknya, proses dekripsi dilakukan dengan mengurangi angka ciphertext dengan kunci dan memodulokannya dengan 10 untuk mendapatkan kembali *plaintext*. Metode ini dinilai sangat aman karena kunci yang digunakan memiliki sifat acak dan unik, sehingga tidak dapat ditebak oleh pihak mana pun. Namun, keberhasilan OTP dalam melindungi sistem sangat bergantung pada faktor-faktor seperti keacakan dan keunikan kode yang dihasilkan, sinkronisasi waktu yang akurat, kecepatan pengiriman kode, serta keamanan dalam proses validasi. Hal ini menegaskan pentingnya penerapan pendekatan yang komprehensif dan berlapis untuk memastikan efektivitas metode OTP dalam mengatasi berbagai ancaman keamanan siber. *E-Wallet* ini dibuat sesederhana mungkin agar user dapat dengan mudah menggunakan *E-Wallet* tersebut. Adapun tampilan *E-Wallet* ini terdiriri dari :

3.1.1 Tampilan Halaman Utama

Halaman utama merupakan halaman yang digunakan untuk akses masuk ke dalam *E-Wallet*. Di sinilah pengguna akan memulai proses login untuk mengakses berbagai fitur dan layanan yang disediakan oleh *E-Wallet*. Gambar 11 merupakan tampilan dari halaman utama, dimana terdapat memasukkan Email dan password. Jika belum memiliki akun bisa registrasi terlebih dahulu.



Gambar 11. Halaman Utama

EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647
Website: https://journal.fkpt.org/index.php/Explorer DOI: https://doi.org/10.47065/explorer.v5i1.1817

3.1.2 Tampilan Halaman *Signup*

Halaman signup ini berfungsi sebagai tempat bagi pengguna untuk membuat akun e-wallet mereka yang baru. Di halaman ini, pengguna akan melalui proses pendaftaran untuk mendapatkan akses ke berbagai fitur dan layanan yang ditawarkan oleh e-wallet. Gambar 12 merupakan tampilan dari halaman *signup*

Gambar 12. Tampilan Halaman *Signup*

3.1.3 Tampilan Halaman *Home*

Halaman *home* merupakan halaman yang menampilkan semua tentang akun pengguna seperti, nama akun, saldo, dan riwayat transaksi. Gambar 13 merupakan tampilan halaman *home*

Gambar 13. Tampilan Halaman *Home*

3.1.4 Tampilan Halaman Daftar Pengguna

Halaman daftar pengguna merupakan halaman yang digunakan untuk memilih kepada siapa user akan mengirim. Gambar 14 merupakan tampilan halaman daftar pengguna

Gambar 14. Tampilan Halaman Daftar Pengguna

EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647
Website: https://journal.fkpt.org/index.php/Explorer DOI: https://doi.org/10.47065/explorer.v5i1.1817

3.1.5 Tampilan Halaman Tambah Pengguna

Halaman signup ini berfungsi sebagai tempat bagi pengguna untuk membuat akun *E-wallet* mereka yang baru. Di halaman ini, pengguna akan melalui proses pendaftaran untuk mendapatkan akses ke berbagai fitur dan layananyang ditawarkan oleh *E-wallet*. Gambar 15 merupakan tampilan dari halaman *signup E-wallet*.

Gambar 15. HalamanTambahPengguna

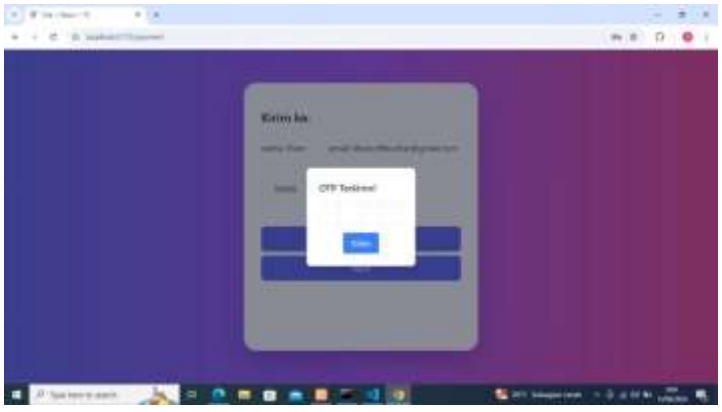
3.1.6 Tampilan Halaman Payment

Halaman *payment* merupakan halaman yang digunakan untuk memasukkan nominal yang akan kita kirim, dan juga memastikan nama akun dan email yang dikirim. Gambar 16 merupakan tampilan halaman *payment*.

Gambar 16. Halaman Payment

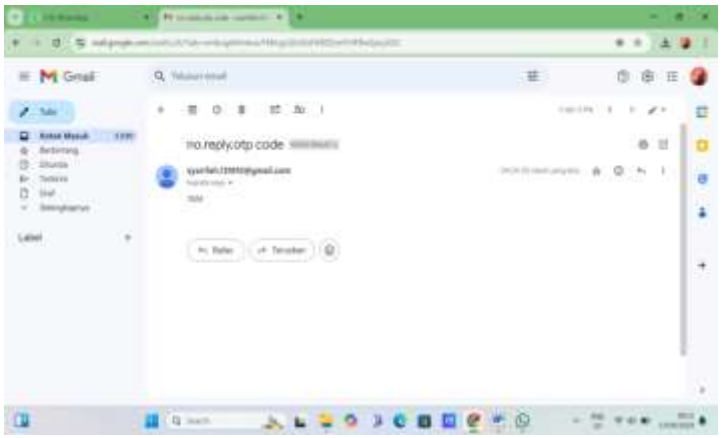
3.1.7 Halaman OTP

Halaman OTP merupakan halaman yang digunakan untuk memasukkan kode OTP yang dikirim sistem ke email pengirim. Gambar 17 dan gambar 18 merupakan tampilan halaman OTP dan kode OTP



Gambar 17. Halaman OTP

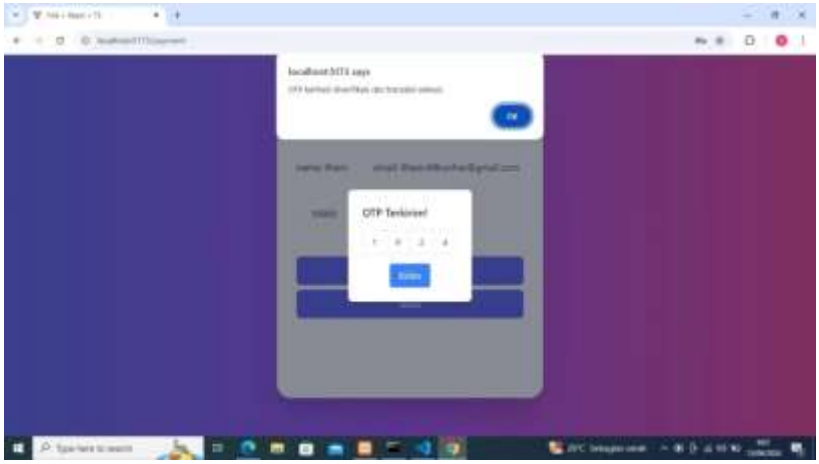
EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647
Website: https://journal.fkpt.org/index.php/Explorer DOI: https://doi.org/10.47065/explorer.v5i1.1817



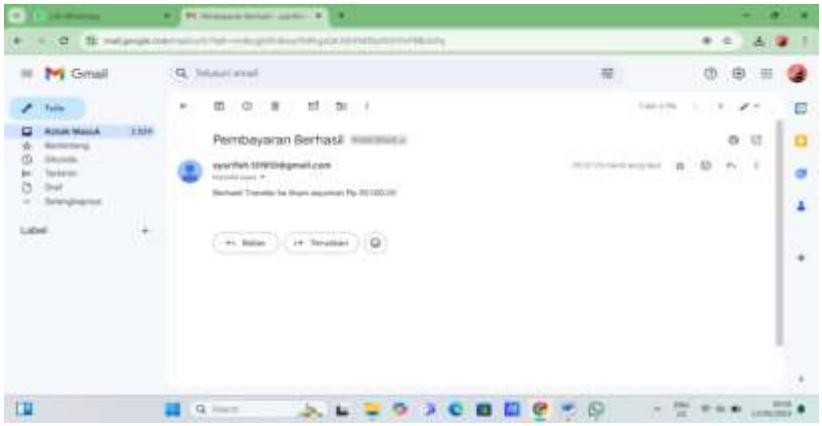
Gambar 18. Kode OTP

3.1.8 Tampilan Halaman Status

Halaman status merupakan halaman yang digunakan untuk mengetahui tentang status pembayaran, apakah pembayaran sukses atau gagal. Gambar 19 merupakan tampilan halaman status dan gambar 20 merupakan notifikasi pembayaran berhasil.



Gambar 19. Halaman Status



Gambar 20. Notifikasi Permbayaran Berhasil

3.2 Metodologi Pengujian

Pengujian ini melibatkan transaksi yang dibagi menjadi dua kategori:

1. Lima transaksi berhasil, dimana OTP yang benar digunakan pada saat transaksi
2. Lima transaksi gagal, dimana OTP yang salah atau sudah kadaluarsa digunakan pada saat transaksi

EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647
Website: https://journal.fkpt.org/index.php/Explorer DOI: https://doi.org/10.47065/explorer.v5i1.1817

3.3 Tabel Pengujian

No.	Nama	Email	Nominal	OTP yang dikirim	Status
1.	Ilham	ilham.tiftkunhar@gmail.com	Rp 100.000	1924	Berhasil
2.	Wahyu	wahyurizkyananda3@gmail.com	Rp.15.000	5317	Berhasil
3.	Listia	listiarizky242002@gmail.com	Rp. 20.000	3353	Berhasil
4.	Riska	riskanoevasari@gmail.com	Rp. 50.000	9190	Berhasil
5.	Adam	adamamarullah10@gmail.com	Rp. 10.000	8158	Berhasil
6.	Zain	Zainrikana8@gmail.com	Rp. 500.000	4222	Gagal
7.	Rosa	rosamelinda004@gmail.com	Rp.10.000	0630	Gagal
8.	Cindy	cindywulandari399@gmail.com	Rp.25.000	1051	Gagal
9.	Maya	mayasariindah092@gmail.com	Rp. 10.000	8569	Gagal
10.	Ega	egaabdinata2002@gmail.com	Rp.12.000	0224	Gagal

3.4 Hasil Pengujian

Hasil pengujian menunjukkan bahwa tidak ada satu pun OTP yang berulang dalam 10 kali transaksi yang dilakukan. Setiap OTP yang dihasilkan unik dan berbeda dari OTP sebelumnya, baik pada transaksi yang berhasil maupun yang gagal. Pengujian ini menunjukkan bahwa sistem OTP pada aplikasi *E-Wallet* telah bekerja dengan baik, dimana setiap transaksi menghasilkan OTP yang unik. Tidak ada OTP yang berulang selama pengujian, yang berarti keamanan dan keunikan OTP pada sistem ini sangat baik, sesuai dengan tujuan dari pengujian ini.

4. KESIMPULAN

Hasil yang telah dilakukan menggunakan metode *One Time Pad* untuk mencegah *cybercrime* memerlukan pendekatan yang komprehensif dan berlapis dengan menyediakan layanan *E-Wallet* secara signifikan meningkatkan keamanan verifikasi akun dan melindungi pengguna dari berbagai ancaman *cybercrime*. Dengan menggunakan algoritma *One Time Pad* yang dimana kunci acak benar-benar tidak diprediksi. Untuk melakukannya enkripsi menambahkan angka plaintext dan kunci, kemudian melakukan mod 10 untuk mendapatkan ciphertext. Sedangkan pada dekripsi mengurangi angka ciphertext dengan kunci, kemudian melakukan operasi mod 10 untuk mendapatkan kembali plaintext. Dengan metode tersebut, sejauh ini sangat aman karena kunci yang digunakan hanya berlaku sekali pakai dan tidak bisa diprediksi oleh pihak mana pun. Kinerja OTP dari segi generator dan validasi sangat bergantung pada beberapa faktor, termasuk keacakan dan keunikan kode yang dihasilkan, sinkronisasi waktu, kecepatan pengiriman, dan keamanan proses validasi. Untuk penelitian selanjutnya, penulis berharap aplikasi ini sudah tersedia secara online dan pengembangan OTP selanjutnya dapat menggunakan saran pengiriman melalui SMS atau *Whatsapp*.

REFERENSI

[1] W. Y. Pradana, M. Irwan, dan P. Nasution, "Keamanan Data Pribadi dalam Penggunaan E-Wallet terhadap Ancaman Cyber Crime," *J. Ekon. dan Bisnis*, vol. 2, no. 2, hal. 345–348, 2024.
[2] R. Ni'mah dan I. Yuliana, "E-Wallet: Sistem Pembayaran Dengan Prinsip Hifzul Maal," *J. Ekon. Syariah*, vol. 5, no. 2, hal. 52–66, 2020, doi: 10.37058/jes.v5i2.2016.
[3] D. F. Harseno, "Analisis Faktor-Faktor Yang Memengaruhi Penggunaan E-Wallet Di Indonesia," *ABIS Account. Bus. Inf. Syst. J.*, vol. 9, no. 4, 2021, doi: 10.22146/abis.v9i4.70384.
[4] A. Sentimen, P. E. Dana, dan D. Gopay, "Analisis Sentimen Penguna E-Wallet Dana Dan Gopay Pada Twitter Menggunakan Metode Support Vector Machine (SVM)," vol. 17, no. x, hal. 323–332, 1978.
[5] U. I. N. Maulana dan M. Ibrahim, "Halaman Sampul Fakultas Psikologi Universitas Islam Negeri Maulana Malik Ibrahim Malang 2020," 2020.
[6] N. E. Saragih, "Implementasi Algoritma One Time Pad pada(Nidia Enjelita Saragih)," *J. Ilm. MATRIK*, vol. Vol.20 No., no. 3, hal. 31–40, 2018.
[7] K. Sukmawati dan D. Kowanda, "Keputusan Penggunaan E-Wallet Gopay Berdasarkan Pengaruh Keamanan, Persepsi Kemudahan Dan Persepsi Manfaat," *J. Ilm. Multidisiplin*, vol. 1, no. 05, hal. 66–72, 2022, doi: 10.56127/jukim.v1i05.481.
[8] A. A. Permana, R. Taufiq, dan R. Destriana, "Implementasi Aplikasi Pengamanan Pesan Gambar Menggunakan Algoritma One Time Pad," *Proceeding SENDIU 2021*, hal. 978–979, 2021.

[9] W. D. A. N. Email, "Mengadopsi kode otp untuk memverifikasi akun aplikasi whatsapp dan email," no. November, hal. 286–292, 2024.
[10] C. Christian, S. H. Sitorus, dan I. Nirmala, "Implementasi Algoritma Rsa Dan One Time Password (Otp) Untuk Pengamanan Data Pengguna Dan Proses Transaksi Pada Website E-Commerce," *Coding J. Komput. dan Apl.*, vol. 11, no. 1, hal. 62, 2023, doi: 10.26418/coding.v11i1.58684.
[11] H. Alam, A. K. Habibi, dan H. Widya, "Penggunaan Algoritma Vigenere Cipher Dan One Time Pad Untuk Keamanan Pesan Teks," *Semin. Nas. Tek. ...*, vol. 5, hal. 160–166, 2022.
[12] O. Dakhi, M. Masril, R. Novalinda, J. Jufrinaldi, dan A. Ambiyar, "Analisis Sistem Kriptografi dalam Mengamankan Data Pesan Dengan Metode One Time Pad Cipher," *INVOTEK J. Inov. Vokasional dan Teknol.*, vol. 20, no. 1, hal. 27–36, 2020, doi: 10.24036/invotek.v20i1.647.
[13] Akhmad Fery Hasanudin dan A Basuki Babussalam, "Perlindungan Hukum Bagi Korban Kejahatan Phising Yang Menguras Saldo M-Banking," *J. Gagasan Huk.*, vol. 6, no. 01, hal. 16–29, 2024, doi: 10.31849/jgh.v6i01.18827.
[14] S. Richiyanti, "Pengaruh dan Penanganan Cybercrime Dalam Perkembangan Teknologi Informasi," *Kodifikasi*, vol. 2, no. 2, hal. 46–56, 2020.
[15] T. Aprilia *et al.*, "Pengaruh Keamanan Two Factor Authentication Terhadap Pencurian Data (Cyber Crime) Pada Media Sosial," *Pengaruh Keamanan Two Factor*, vol. 2, no. 5, hal. 449–458, 2024, [Daring]. Tersedia pada: https://doi.org/10.5281/zenodo.11496678
[16] F. Diani dan Y. Widhiyasana, "Enkripsi SMS dengan Menggunakan One Time Pad (OTP) dan Kompresi Lempel-Ziv-Welch (LZW)," *J. Nas. Tek. Elektro dan Teknol. Inf.*, vol. 7, no. 3, hal. 3–8, 2018, doi: 10.22146/jnteti.v7i3.436.
[17] R. Pratiwi, L. C. Utami, R. Bima Sakti, dan Triase, "Perancangan Keamanan Data Pesan Dengan Menggunakan Metode Kriptografi Caesar Cipher," *Bull. Inf. Technol.*, vol. 3, no. 4, hal. 367–373, 2022, doi: 10.47065/bit.v3i4.420.
[18] O. K. Sulaiman, "Generate Pseudo-Random Numbers Linear-Feedback Shift Register (LSFR) Pada Kunci Algoritma One Time Pad (OTP)," *Semin. Nas. Teknol. Komput. Sains*, hal. 171–175, 2020.