MENGADOPSI KODE OTP UNTUK MEMVERIFIKASI AKUN APLIKASI WHATSAPP DAN EMAIL

Miftah Farid[1], Erna Kumalasari Nurnawati[2*]
[1,2,] Universitas Akprind Indonesia,
e-mail: [1]farid@akprind.ac.id ,[2]ernakumala@akprind.ac.id

ABSTRACT

Usernames and passwords as authentication requirements for a system that are used repeatedly can make account security on that system vulnerable to data theft. Digital application access security is increasingly important, especially with the increase in cyber-attacks against login systems that use statistical passwords. One-Time Password (OTP) is one of the popular security solutions to enhance the login verification layer. This research aims to implement an OTP system on the WhatsApp and email applications as an authentication method. The method used is through experimental web-based application development by sending WhatsApp OTP and email and users are required to verify their identity using the code. Testing was carried out on 10 users by dividing them into two groups who received authentication via WhatsApp and email. The research results show that implementing OTP has succeeded in reducing the risk of unauthorized access by up to 80%. Thus, it is hoped that the use of OTP will effectively increase the security of the login process without involving the user. Thus, it is hoped that this research can contribute to better passcode security.

***Keywords**: Email, OTP, Security Application, Verification, WhatsApp*

INTISARI

Penggunaan *username* dan *password* sebagai syarat otentikasi pada suatu sistem yang digunakan secara berulang dapat membuat keamanan akun pada sistem tersebut menjadi rentan dilakukan pencurian data. Keamanan akses aplikasi digital semakin penting, terutama dengan meningkatnya serangan siber terhadap sistem *login* yang menggunakan kata sandi statistik. *One-Time Password (OTP)* adalah salah satu solusi keamanan populer untuk meningkatkan lapisan verifikasi *login*. Penelitian ini bertujuan untuk mengimplementasikan sistem OTP pada aplikasi *WhatsApp* dan *email* sebagai metode autentikasi. Metode yang digunakan adalah melalui eksperimen pengembangan aplikasi berbasis web dengan pengiriman OTP WhatsApp dan *email* dan pengguna diharuskan memverifikasi identitasnya menggunakan kode tersebut. Pengujian dilakukan terhadap 10 pengguna dengan membagi dalam dua kelompok yang menerima otentifikasi melalui *WhatsApp* dan *email*. Hasil penelitian menunjukkan bahwa penerapan OTP berhasil mengurangi risiko akses tidak sah hingga 80%. Dengan demikian diharapkan penggunaan OTP efektif meningkatkan mengamankan proses *login* tanpa melibatkan pengguna. Dengan demikian diharapkan Penelitian ini dapat memberikan kontribusi dalam pengamanan kode sandi dengan lebih baik.

Kata kunci: Aplikasi Keamanan, Email, OTP, Verifikasi, WhatsApps,

1. PENDAHULUAN

Salah satu bentuk verifikasi dua faktor yang paling umum digunakan adalah *One Time Password (OTP)*. OTP adalah kode yang hanya berlaku untuk satu sesi atau transaksi *login*, sehingga sangat mengurangi kemungkinan akses yang tidak sah. Pengiriman OTP melalui *platform* pesan instan seperti *WhatsApp* dan *Email* telah menjadi semakin populer dalam beberapa tahun terakhir. Hal ini disebabkan oleh jumlah pengguna yang besar dan infrastruktur yang dapat diandalkan untuk pengiriman pesan cepat yang dimiliki oleh kedua *platform* tersebut. Salah satu hal penting yang harus diperhatikan oleh para pengembang adalah keamanan aplikasi digital mereka. Meningkatnya jumlah pengguna internet dan aplikasi mobile meningkatkan potensi serangan siber. Verifikasi dua faktor, adalah salah satu cara yang efektif untuk meningkatkan keamanan aplikasi karena memerlukan dua jenis informasi untuk mengautentikasi pengguna yang diketahui seperti password dan perangkat yang yang dimiliki seperti perangkat seluler (Nasution, A. B., Hrp, A. Y. N., Yudi, Y., & Fauzi, M., 2024). Penggunaan OTP diklaim dapat mengatasi keamanan login. Password yang sebelumnya menggunakan satu *username* dan satu *password* akan ditambahkan lagi dengan satu *password* random yang dikirim ke ponsel pengguna saat login (Danrich U.

Balasta, Stacy Marie, C. Pelito, 2022). Studi ini menemukan bahwa pembuatan sistem login seperti ini sangat penting untuk memastikan bahwa orang dapat mengakses layanan yang berbasis web, lokal, atau aplikasi dengan aman. Semakin banyak layanan yang menggunakan fasilitas ini, semakin sedikit kasus yang merugikan banyak pihak, baik materi maupun emosional. Setelah kata sandi statis yang dimasukkan pada halaman login dimasukkan ke database, server membuat kata sandi acak, yang kemudian dikirimkan ke ponsel pengguna. Nomor telepon yang terdaftar dalam database digunakan untuk mengirimkan (D. E. Kurniawan, M. Iqbal, J. Friadi, F. Hidayat, and R. D. Permatasari, 2021).

Menurut (Pratama, 2019), keamanan komputer meliputi beberapa aspek, yaitu 1) Authentication: agar penerima informasi dapat memastikan keaslian pesan tersebut datang dari orang yang dimintai informasi. Dengan kata lain informasi tersebut benar-benar dari orang yang dikehendaki.2). Integrity: keaslian pesan yang dikirim melalui sebuah jaringan dan dapat dipastikan bahwa informasi yang dikirim tidak dimodifikasi oleh orang yang tidak berhak dalam perjalanan informasi tersebut 3) Authority: informasi yang berada pada sistem jaringan tidak dapat dimodifikasi oleh pihak yang tidak berhak atas akses tersebut 4) Confidentiality: merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses 5) Privacy: merupakan lebih ke arah data-data yang sifatnya pribadi 6) Availability: aspek availability atau ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan 7) Acces control: aspek ini berhubungan dengan cara pengaturan akses kepada Informasi.

OTP adalah kode rahasia yang hanya dapat digunakan satu kali dalam sesi *login* atau transaksi tertentu. Pengguna menerima kode OTP melalui media komunikasi yang telah diverifikasi, seperti *WhatsApp* atau *email*. OTP sering kali diterapkan untuk mencegah serangan *brute force, phishing*, dan peretasan lainnya yang mengeksploitasi kelemahan pada kata sandi statis. OTP berupa kode acak yang hanya berlaku untuk satu sesi login atau transaksi. Teknologi OTP telah digunakan secara luas sebagai metode autentikasi kedua dalam sistem 2FA. OTP menawarkan keamanan yang lebih baik karena kode ini hanya berlaku dalam waktu yang sangat terbatas dan tidak dapat digunakan lagi (Kaya, 2024). Sistem login yang kuat adalah kunci utama untuk melindungi data dan identitas pengguna dari akses yang tidak sah. Implementasi OTP sebagai metode autentikasi tambahan terbukti mampu meningkatkan perlindungan terhadap serangan siber. Berdasarkan Penelitian dari (Wicaksono, 2019), sistem yang hanya mengandalkan kata sandi rentan terhadap berbagai macam serangan, termasuk *phishing* dan *keylogging*. Dalam pembuatan OTP (*OTP generate*) terdapat 3 pendekatan, yaitu a. berdasarkan *"time-synchronization"* antara otentikasi *server-client* yang menyediakan p*assword* Dimana OTP akan bersifat valid bila dalam peride waktu yang singkat b. berdasarkan *"mathematical algorithm"* yang memungkinkan generalisasi suatu password baru berdasarkan password sebelumnya dan c. berdasarkan *"mathematical algorithm"* Dimana *password* ditentukan secara random (Danrich U. Balasta, Stacy Marie, C. Pelito, 2022).

Penelitian yang dilakukan oleh (E.K Nurnawati, MR Thaariq, RY Ariyana, 2023) menyatakan bahwa Perancangan otentikasi OTP menggunakan kode unik via email yang dapat digunakan sebagai alternatif pengamanan untuk masuk ke suatu sistem karena pengguna hanya mendapatkan satu kali kode setiap akan memasuki sistem. Hal ini dapat diterapkan pada sistem informasi baik sistem berbasis desktop, sistem berbasis web maupun sistem berbasis perangkat bergerak. Penggunaan OTP via email juga menjamin pengguna harus mendaftarkan email kepada sistem, sehingga menambah keamanan dalam penggunaan sistem. Sedangkan pada penelitian yang dilakukan oleh (Rayan Abdulrahim Al-Sahli and Abdulrahman Al-Mutairi, 2024) menjelaskan bagaimana melakukan pengamanan autentifikasi sistem dengan multi-faktor autentitikasi. Sedangkan Penelitian yang dilakukan oleh (Chairil Anwar and Sriani, 2024) juga telah mengimplementasikan penggunaan OTP dengan algoritma HMAC dengan dua faktor untuk mengamankan sistem login relawan pemilu.

Tujuan penelitian ini adalah untuk membuat model sistem keamanan *password* dengan metode OTP agar pengguna dapat mengakses web dengan lebih aman serta melakukan evaluasi penggunannya dari suatu sistem. Penggunaan OTP yang menggunakan metode Dimana kode hanya berlaku untuk satu kali digunakan oleh user. Aplikasi ini ditujukan untuk melindungi penggunaan *password* dari bahaya dari teknik *phishing*. Implementasi OTP melalui WhatsApp menawarkan beberapa keuntungan, seperti kemudahan penggunaan dan kecepatan pengiriman. Namun, ada beberapa masalah yang perlu diperhatikan, seperti ketergantungan pada koneksi internet dan kemungkinan pembatasan WhatsApp.

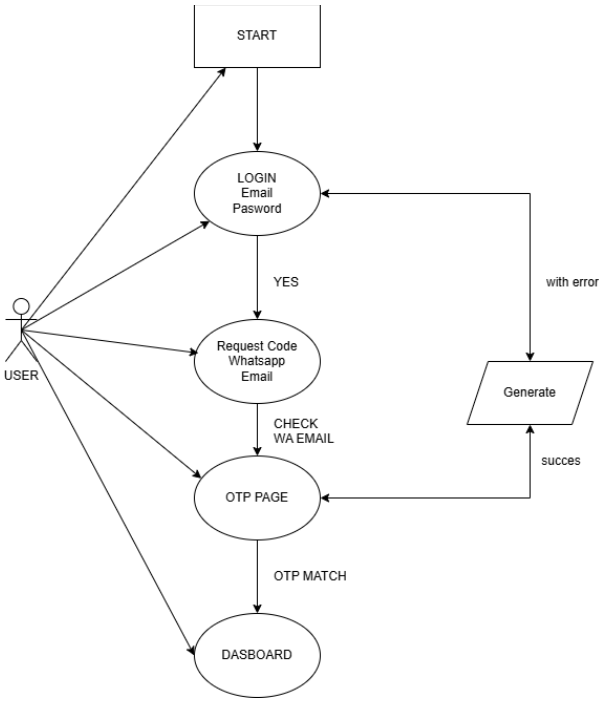
2. METODE PENELITIAN

Metode yang digunakan dalam penelitian ini meliputi :

a. Perancangan Sistem OTP
   Pada tahap ini, analisis dilakukan untuk menentukan bagian dan fungsi sistem verifikasi OTP yang diperlukan. Ini termasuk kebutuhan fungsional seperti login, pengiriman OTP, verifikasi OTP, dan manajemen pengguna, serta kebutuhan non-fungsional seperti keamanan, kecepatan pengiriman, dan

keandalan sistem. Arsitektur sistem bertujuan untuk memungkinkan aplikasi web berintegrasi dengan API *WhatsApp*. Arsitektur ini mencakup *backend server* yang menangani permintaan pengguna, mengelola pengiriman dan verifikasi OTP, WhatsApp API yang mengirimkan OTP ke pengguna, dan database yang menyimpan informasi pengguna, OTP yang dibuat, dan status verifikasi.

Pada gambar 1 dijelaskan bagaimana diagram alir perancangan sistem penerapan OTP pada suatu sistem, dimana pengguna akan melakukan login ke email, lalu akan melakukan permintaan kode melalui *WhatsApp Mail.* Lalu dilanjutkan dengan Pengecekan OTP. Pada saat dilakukan permintaan ini, maka OTP Page akan membangkitkan satu kali kata kunci yang akan dikirimkan melalui *WhatsApp.*



Gambar 1. Alur Kerja Sistem

Alur proses sistem dapat dijelaskan dengan langkah sebagai berikut:

Langkah 1 - *Login Request*:
Pengguna memasukkan email dan password pada halaman login.

Langkah 2 - Cek Validitas *Email* dan *Password*:
Backend memverifikasi apakah email terdaftar di database.
Jika *email* ditemukan, sistem memverifikasi apakah *password* yang dimasukkan benar.
Jika *email* atau *password* tidak valid, pengguna akan menerima pesan kesalahan.

Langkah 3 - *Request OTP*:
Jika *email* dan *password valid*, pengguna diarahkan ke tahap permintaan OTP.
Sistem *backend* akan menghasilkan kode OTP secara acak.

Langkah 4 - Pengiriman OTP:
OTP dikirimkan ke pengguna melalui *WhatsApp API* atau *SMTP server* untuk *email*, tergantung pilihan pengguna.

Langkah 5 - *OTP Verification*:
Pengguna akan memasukkan kode OTP pada halaman verifikasi.
Sistem memverifikasi apakah OTP yang dimasukkan sesuai dan masih berlaku.
Jika OTP *valid*, akses ke dashboard diberikan. Jika tidak valid atau sudah kadaluwarsa, pengguna menerima pesan error.

Langkah 6 - Akses *Dashboard*:
Setelah berhasil verifikasi OTP, pengguna diarahkan ke halaman *dashboard*

b. Pengujian Penggunaan OTP

Pengujian dilakukan dengan melibatkan 10 pengguna yang dibagi menjadi dua kelompok: 5 pengguna menerima OTP melalui WhatsApp, dan 5 pengguna melalui email. Setiap pengguna akan mencoba login dan memasukkan OTP yang diterima. Tingkat keberhasilan pengiriman dan verifikasi OTP dianalisis

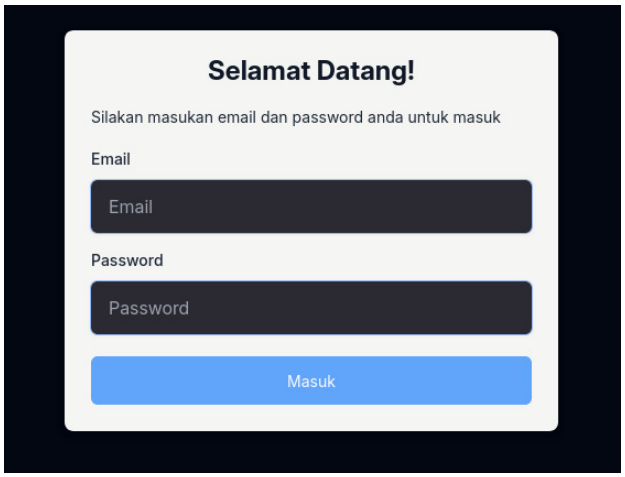
Penelitian ini menggunakan *Framework Backend: Remix, API WhatsApp: WABLAS, SMTP Server* dan untuk

pengiriman OTP melalui email menggunakan *Frontend Remix*.

3. HASIL DAN PEMBAHASAN

a. Implementasi Sistem

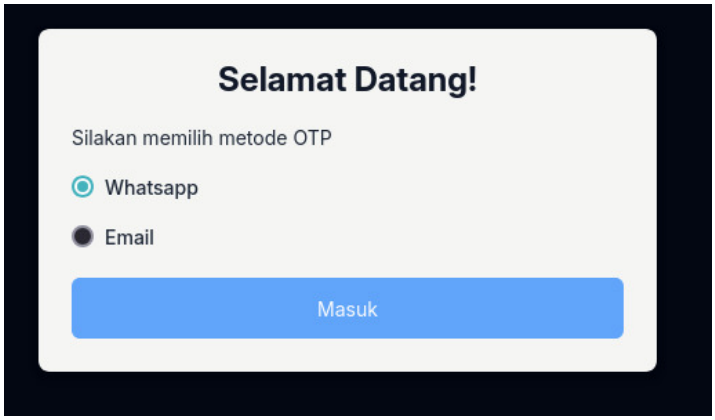
Sistem ini menggunakan *Framework Backend Remix*, dengan *API WhatApp WAblas, SMTP Server, Frontend Remix*. Dengan menggunakan *browser* , desain program ditampilkan. Dalam hal ini digunakan *browser* yaitu mozila firefox. Tampilan halaman utama website dalam penelitian ditunjukkan pada Gambar 2.



Gambar 2. Halaman Login sebelum OTP

b. Pengiriman dan penerimaan OTP

Sistem OTP berhasil diimplementasikan dan diuji. Waktu pengiriman OTP melalui *WhatsApp* lebih cepat dibandingkan dengan *email.* Rata-rata waktu pengiriman OTP melalui *WhatsApp* adalah 4 detik, sedangkan *email* membutuhkan waktu 12 detik. Laman pilihan pengiriman disajikan pada Gambar 3.

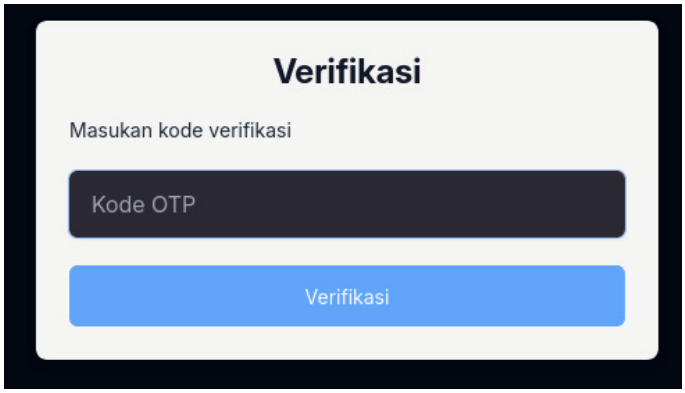


Gambar 3. Pemilihan jenis OTP

c. Pengamanan Sistem

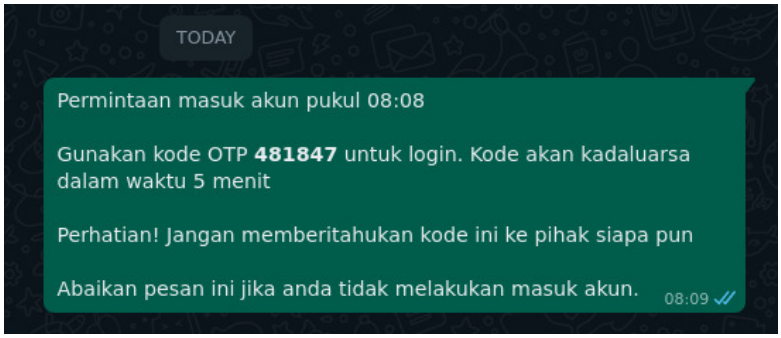
Pengujian penetrasi dilakukan untuk menemukan kemungkinan kerentanan sistem. Hasil pengujian menunjukkan bahwa sistem memiliki tingkat keamanan yang tinggi dan memiliki mekanisme untuk melindunginya dari serangan *brute force* dan *man-in-the-middle (MITM).* Selain itu, penggunaan OTP yang berlaku hanya untuk satu sesi *login* membantu mencegah akses yang tidak sah (A. Senol, G. Acar, M. Humbert, and F. Z. Borgesius, 2022). Gambar 4 menunjukkan permintaan verifikasi OTP.

P - ISSN: 1979-911X
E - ISSN: 2541-528X



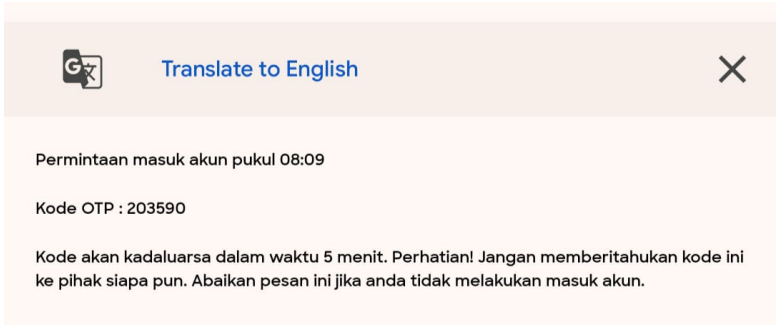
Gambar 4. Verifikasi memasukan Kode OTP

d. Penerimaan OTP pada akun *WhastApp*
Penerimaan OTP yang diperoleh pada akun *WhastApp* disajikan pada Gambar 5. Pada pesan diberikan waktu limitasi pemakaian dan peringatan keamanan.

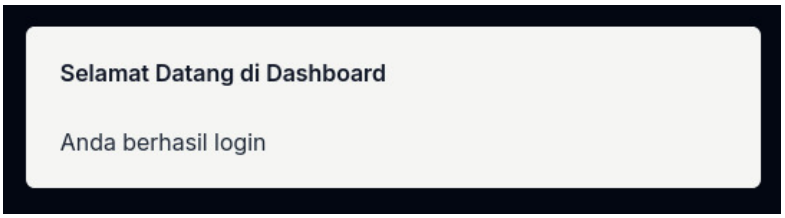


Gambar 5. Penerimaa Kode OTP WhatsApp

e. Penerimaan OTP di akun Email
Sedangkan pada penerimaan OTP melalui *email* disajikan pada gambar 6. Pengiriman juga disertai dengan limitasi waktu dan peringatan pengamanan. Apabila telah berhasil melakukan login maka akan diberikan pesan sebagaimana disajikan pada Gambar 7.

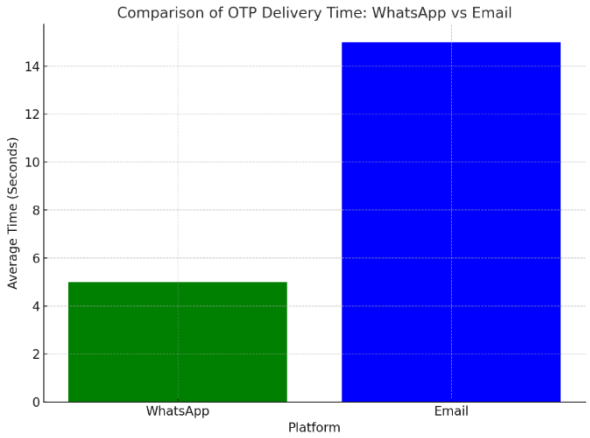


Gambar 6. Penerimaan Kode OTP *Email*



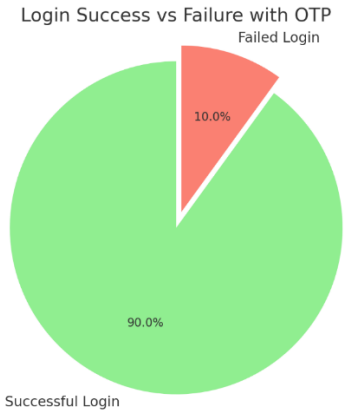
Gambar 7. Berhasil Login di *Dashboard*

Pada gambar 8, diberikan analisis perbandingan waktu yang diperlukan dalam pengiriman OTP melalui *Email* dan *WhastApp.*



Gambar 8. Grafik Perbandingan Waktu Pengiriman OTP melalui WhatsApp dan Email

Waktu yang dipelukan oleh 10 user yang dilakukan pengujian adalah rata-rata 5.1 detik, sedangkan pengiriman OTP melalui email lebih lambat yaitu mencapai 14.8 detik. Hal ini mencerminkan pengiriman melalui *WhastApp* lebih efisien dari segi waktu. Sedangkan pada gambar 7, disajikan hasil kinerja OTP yang dikirimkan, dimana 90% OTP yang diberikan berhasil digunakan untuk melakukan *login*.



Gambar 9. Grafik Keberhasilan dan Kegagalan *Login* dengan OTP

4. KESIMPULAN

Implementasi One Time Password (OTP) untuk otentikasi login melalui *WhatsApp* dan *email* terbukti mampu meningkatkan keamanan akun pengguna secara signifikan. Penggunaan OTP tidak hanya meningkatkan keamanan tetapi juga memberikan kenyamanan bagi pengguna dalam proses login. Pengiriman OTP melalui *WhatsApp* lebih cepat dibandingkan dengan *email*, namun keduanya memberikan tingkat keberhasilan verifikasi yang tinggi. Sistem OTP ini diharapkan dapat diadopsi oleh pengembang aplikasi untuk meningkatkan keamanan tanpa mengurangi kenyamanan pengguna.

5. UCAPAN TERIMAKASIH

Para penulis mengucapkan Terimakasih kepada DP2M dan Rektor Universitas AKPRIND Indonesia yang telah mendanai Penelitian ini.

DAFTAR PUSTAKA

A. Senol, G. Acar, M. Humbert, and F. Z. Borgesius. (2022). Leaky Forms: A Study of Email and Password Exfiltration Before Form Submission. *Proceedings of the 31st USENIX Security Symposium*, (pp. 1813–1830).

Chairil Anwar and Sriani. (2024, 9 30). Implementasi Algoritma OTP dan HMAC untuk TwoFactor

Authentication Sistem Login Relawan Pemilu. *Jurnal Teknika*, 83-94.

D. E. Kurniawan, M. Iqbal, J. Friadi, F. Hidayat, and R. D. Permatasari. (2021). Login Security Using One Time Password (OTP) Application with Encryption Algorithm Performance. *Journal of Physics Conf Series, 1783*(1). doi:10.1088/1742-6596/1783/1/012041.

Danrich U. Balasta, Stacy Marie, C. Pelito. (2022, June). Enhancement of Time-Based One-Time Password for. *International Journal of Innovative Science and Research Technology, 7*(6). Retrieved from https://www.ijisrt.com/assets/upload/files/IJISRT22JUN522.pdf

E.K Nurnawati, MR Thaariq, RY Ariyana. (2023). Perancangan Otentikasi One Time Password menggunakan Kode Unik via Email. *Jurnal Dinamika Informatika*, 70-78.

Kaya, D. (2024, June). *Implementing WhatsApp OTP: A Comprehensive Guide*. Retrieved from D.DAT: https://d-dat.com/implementing-whatsapp-otp-a-comprehensive-guide/

Nasution, A. B., Hrp, A. Y. N., Yudi, Y., & Fauzi, M. (2024). Implementation of OTP Code as Application Login Verification Via Whatsapp. *Indonesian Journal of Applied and Industrial Sciences (ESA), 3*(4), 395–402. doi:https://doi.org/10.55927/esa.v3i4.10225

Pratama. (2019). *Integrasi API WhatsApp untuk Pengiriman OTP dalam Sistem Verifikasi.* Yogyakarta: Gadjah Mada Press.

Rayan Abdulrahim Al-Sahli and Abdulrahman Al-Mutairi. (2024). *Secure Authentication System based on Multi-Factor Authentication.* Taibah University. doi:10.13140/RG.2.2.24880.74247

Wicaksono. (2019). *Penggunaan OTP dalam Sistem Login untuk Meningkatkan Keamanan Aplikasi.* Surabaya: Universitas Negeri Surabaya.