

Pengembangan Sistem Validasi Keabsahan Invoice Dengan Integrasi QR Code Dan Algoritma TOTP (Studi Kasus: CV. Mandiri Bersama)

Fildzah Attira Khair^{*1}, Fawwaz Ali Akbar², Eka Prakarsa Mandyartha³

^{1,2,3}Program Studi Informatika, Fakultas Ilmu Komputer, UPN “Veteran” Jawa Timur

E-mail: ^{*1}21081010148@student.upnjatim.ac.id,

²fawwaz.ali.fik@upnjatim.ac.id, ³eka_prakarsa.fik@upnjatim.ac.id

Abstrak

Sistem validasi keabsahan invoice sangat penting dalam dunia bisnis untuk mencegah pemalsuan dokumen dan memastikan transaksi yang sah. Penelitian ini mengembangkan sistem berbasis web yang mengintegrasikan Quick Response (QR) Code dan algoritma Time-based One-Time Password (TOTP) untuk meningkatkan keamanan dan keabsahan invoice pada CV. Mandiri Bersama. QR Code digunakan untuk memberikan akses cepat dan langsung ke informasi invoice, sementara algoritma TOTP digunakan untuk mengotentikasi pengguna yang berwenang dengan kode unik yang terus berubah dalam interval tertentu. Sistem ini juga menerapkan metode Two-Factor Authentication (2FA) dengan kombinasi email dan OTP yang dihasilkan menggunakan algoritma TOTP, memastikan bahwa hanya pengguna yang memiliki akses email yang sah yang dapat melakukan validasi invoice. Dengan penerapan sistem ini, proses validasi invoice menjadi lebih aman, akurat, dan efisien. Hasil implementasi menunjukkan bahwa QR Code dapat dimanfaatkan untuk memvalidasi keabsahan invoice dengan cepat dan efisien, sementara OTP dari algoritma TOTP dapat menjaga keamanan akses invoice dengan memastikan hanya pengguna yang berhak yang dapat melakukan verifikasi, sehingga mengurangi risiko manipulasi atau penyalahgunaan dokumen.

Kata Kunci—Invoice, QR Code, TOTP, 2FA, Keabsahan

Abstract

Invoice validation system is very important in the business world to prevent document forgery and ensure legitimate transactions. This research develops a web-based system that integrates Quick Response (QR) Code and Time-based One-Time Password (TOTP) algorithm to improve the security and validity of invoices at CV. Mandiri Bersama. QR Code is used to provide quick and direct access to invoice information, while TOTP algorithm is used to authenticate authorized users with a unique code that keeps changing in a certain interval. The system also implements the Two-Factor Authentication (2FA) method with a combination of email and OTP generated using the TOTP algorithm, ensuring that only users with authorized email access can validate invoices. With the implementation of this system, the invoice validation process becomes more secure, accurate, and efficient. The implementation results show that QR codes can be utilized to validate the validity of invoices quickly and efficiently, while OTP from the TOTP algorithm can maintain the security of invoice access by ensuring that only authorized users can verify, thus reducing the risk of document manipulation or misuse.

Keywords—Invoice, QR Code, TOTP, 2FA, Validation

1. PENDAHULUAN

Dalam dunia bisnis, salah satu jenis dokumen yang sering digunakan adalah invoice. Invoice berperan penting sebagai dokumen yang berisikan catatan atau detail transaksi antara penjual dengan pembeli. Seiring dengan kemajuan teknologi informasi, pemalsuan dokumen semakin mudah dilakukan oleh pihak-pihak yang tidak berkepentingan. Biasanya, pemalsuan dokumen dilakukan dengan cara memodifikasi isi atau membuat dokumen baru yang meniru tampilan dokumen asli [1]. Tanda tangan merupakan representasi asli dari sebuah identitas yang bersifat legal dan tidak boleh digunakan tanpa sepengetahuan pemilik identitas. Keberadaan tanda tangan pada sebuah dokumen menunjukkan bahwa pihak yang menandatangani telah menyetujui atau mengesahkan isi dokumen [2]. Meski begitu, kejahatan pemalsuan tanda tangan masih banyak terjadi. Berlaku juga dengan stempel perusahaan, dengan kemudahan teknologi, pemalsuan stempel menjadi ancaman yang nyata.

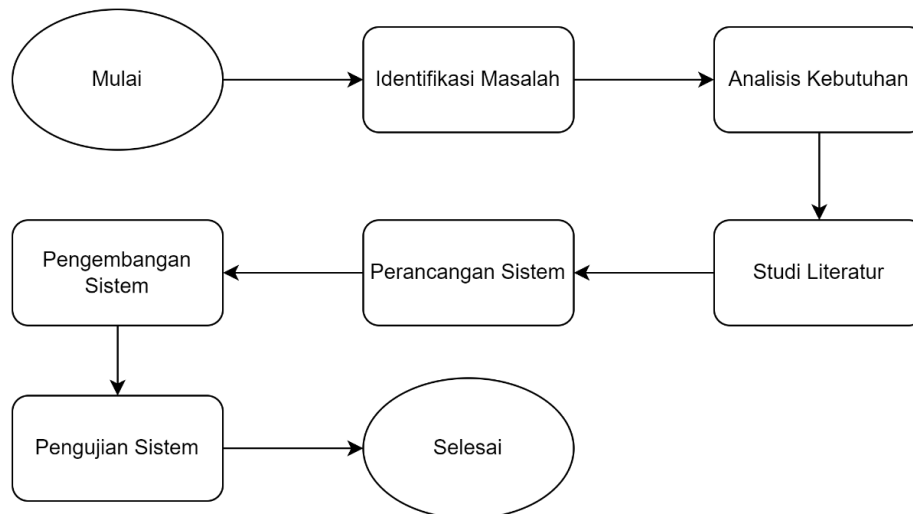
CV. Mandiri Bersama adalah perusahaan forwarding consultant yang mengelola logistik dan konsultasi pengiriman. Invoice berperan penting sebagai bukti transaksi yang harus dijaga keasliannya. Saat ini, QR code yang digunakan hanya mengarahkan pengguna ke kontak perusahaan untuk validasi secara manual, sehingga kurang efisien dalam proses operasional perusahaan. Oleh karena itu, diperlukan sistem yang dapat memvalidasi keabsahan invoice secara otomatis melalui QR code. *Quick Response* atau QR code adalah barcode dua dimensi yang mampu menyimpan data di dalamnya. QR code telah banyak digunakan karena memiliki berbagai fitur unggulan, seperti data yang berkapasitas besar, kecepatan pemindaian tinggi, dan ukuran cetak yang kecil [3]. Pengguna dapat mengakses informasi dalam QR code dengan memindainya menggunakan perangkat seperti smartphone atau scanner. Proses ini praktis, tetapi juga rentan terhadap akses tidak sah. Oleh karena itu, diperlukan keamanan tambahan untuk memastikan hanya pihak berwenang yang dapat mengakses data, terutama pada dokumen atau transaksi sensitif.

Dengan memanfaatkan autentikasi, keamanan dapat ditingkatkan. Autentikasi adalah bukti yang diberikan oleh pengguna untuk memastikan kepada sistem bahwa ia benar-benar sesuai dengan identitas yang telah diberikan. Sesuatu yang dimiliki pengguna merupakan salah satu faktor autentikasi pengguna yang dapat digunakan. Ini melibatkan objek fisik atau digital yang hanya dimiliki oleh pengguna. Terdapat juga sesuatu yang diketahui pengguna yang juga termasuk kedalam salah satu faktor autentikasi yang dapat digunakan, sesuatu yang diketahui pengguna melibatkan informasi spesifik yang hanya diketahui oleh pengguna seperti password, PIN code, atau nama gadis ibu [4]. Oleh karena itu, proses validasi ini dapat diintegrasikan dengan metode autentikasi tambahan seperti Two Factor Authentication atau 2FA yang merupakan autentikasi dengan mengkombinasikan dua atau lebih faktor autentikasi untuk meningkatkan keamanan [5].

Selain sebagai pengganti dari tanda tangan atau stempel perusahaan, QR code digunakan untuk membantu proses validasi keabsahan invoice yang diterbitkan oleh CV. Mandiri Bersama kepada klien mereka. Dengan itu, klien dapat memindai QR code yang ada untuk memvalidasi apakah invoice yang mereka terima mempunyai detail yang sama dengan informasi yang disediakan dalam QR code tersebut. Penerapan metode autentikasi 2FA ada dengan memanfaatkan sesuatu yang dimiliki pengguna yaitu email dan sesuatu yang diketahui pengguna yaitu one time password atau OTP yang didapatkan pengguna melalui email yang dimana OTP tersebut dibangkitkan dari algoritma Time based One-Time Password atau TOTP [6]. Pembuatan invoice di CV. Mandiri Bersama masih dilakukan secara manual menggunakan *worksheet*, yang memakan waktu, rentan terhadap kesalahan, dan tidak memiliki format standar. Oleh karena itu, sistem yang dikembangkan tidak hanya mencakup validasi keabsahan invoice, tetapi juga fitur pembuatan invoice dengan QR code terintegrasi untuk memastikan keabsahan dokumen.

2. METODE PENELITIAN

2.1. Alur Penelitian



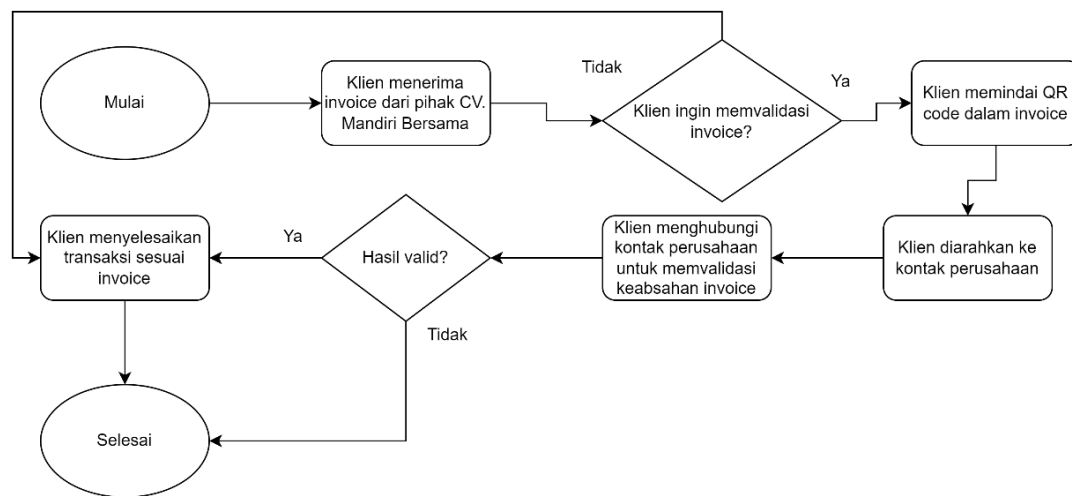
Gambar 1 Alur Penelitian

Pada Gambar 1 menampilkan tahapan pengembangan sistem yang mencakup beberapa langkah utama. Proses dimulai dengan identifikasi masalah, di mana permasalahan utama dalam sistem saat ini dianalisis untuk menemukan kesenjangan yang perlu diperbaiki. Selanjutnya, dilakukan analisis kebutuhan guna menentukan fitur dan fungsi yang dibutuhkan sistem agar dapat meningkatkan efisiensi serta kualitas layanan. Setelah itu, studi literatur dilakukan untuk memahami teori dan penelitian sebelumnya yang relevan sebagai dasar pengembangan.

Berdasarkan hasil analisis tersebut, tahap perancangan sistem mulai dilakukan dengan mendesain arsitektur sistem serta dokumentasi teknis yang akan digunakan dalam implementasi. Proses berlanjut ke pengembangan sistem, yang mencakup pengkodean, pengujian awal, serta pemeliharaan agar sistem dapat berfungsi dengan optimal. Tahapan akhir adalah pengujian sistem, di mana metode blackbox testing digunakan untuk memastikan bahwa setiap fitur berjalan sesuai spesifikasi tanpa melihat struktur kode internal. Pengujian ini memastikan bahwa sistem dapat memenuhi kebutuhan pengguna dengan baik sebelum diterapkan sepenuhnya.

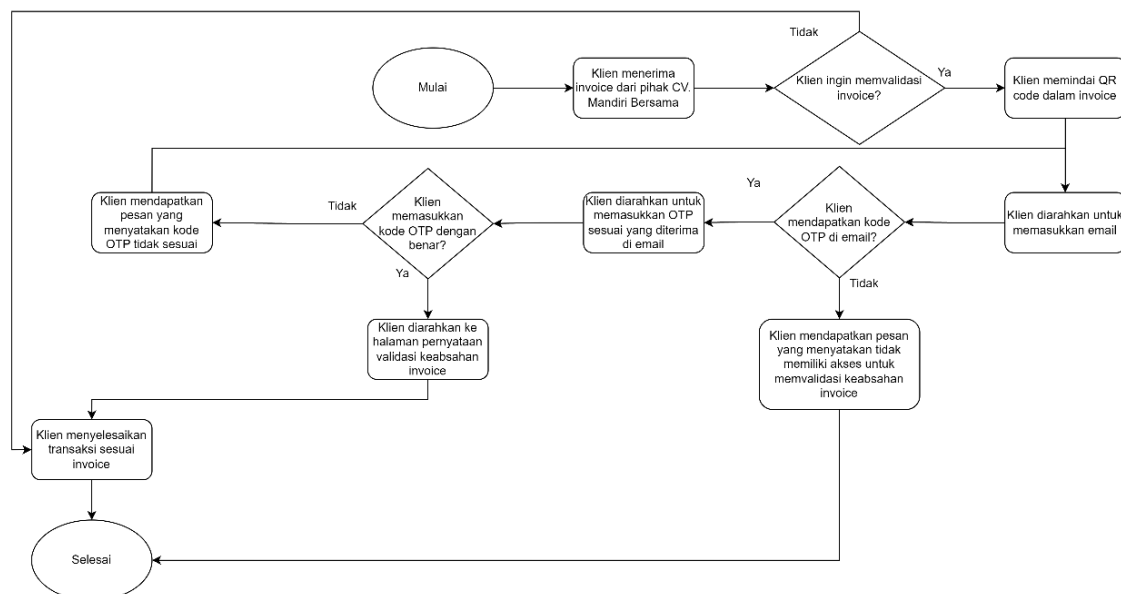
2.2. Alur Proses Bisnis

Perlu diketahui juga alur proses bisnis dari sisi klien CV. Mandiri Bersama tersedia pada Gambar 2 dalam memvalidasi keabsahan invoice saat ini dimulai ketika klien menerima invoice. Jika klien ingin memvalidasi keabsahan invoice yang diterima, mereka dapat memindai kode QR yang tersedia di invoice. Jika klien tidak ingin memvalidasi keabsahan invoice yang diterima, mereka dapat langsung menyelesaikan transaksi yang ada. Pemindaian QR code ini akan mengarahkan klien ke kontak perusahaan untuk melakukan konfirmasi. Setelah menghubungi perusahaan dan memastikan bahwa invoice tersebut valid, klien bisa melanjutkan transaksi sesuai dengan invoice tersebut.



Gambar 2 Alur Proses Bisnis Klien Dalam Validasi Keabsahan Invoice

Pada Gambar 3 menampilkan alur proses bisnis nantinya setelah penerapan sistem validasi keabsahan invoice di CV. Mandiri Bersama. Proses dimulai ketika klien menerima invoice dan memindai QR code yang tertera untuk melakukan validasi. Setelah pemindaian, klien akan diarahkan ke halaman sistem dan diminta memasukkan email yang telah terdaftar. Sistem kemudian mengirimkan kode OTP hasil algoritma TOTP ke email klien sebagai langkah verifikasi tambahan. Jika email tidak terdaftar atau klien gagal menerima OTP, sistem akan menolak akses. Sebaliknya, jika OTP dimasukkan dengan benar, klien akan diarahkan ke halaman validasi yang menampilkan keabsahan invoice. Jika OTP salah, sistem akan menampilkan pesan kesalahan. Dengan sistem ini, proses validasi menjadi lebih aman dan cepat, memastikan hanya pengguna dengan email terdaftar yang dapat mengakses informasi invoice. Selain itu, sistem ini juga melindungi halaman validasi dari akses tidak sah, meminimalkan risiko pemalsuan atau penyalahgunaan invoice.



Gambar 3 Alur Proses Bisnis Klien Menggunakan Sistem Validasi Keabsahan Invoice

Selain elemen validasi, CV. Mandiri Bersama menghadapi kendala lain karena proses pembuatan *invoice* masih dilakukan juga secara manual menggunakan aplikasi *worksheet*. Beberapa kelemahan pendekatan manual ini termasuk kurangnya standar format yang seragam, risiko kesalahan pengetikan yang tinggi serta ketidakefisienan dalam menyusun dokumen. Selain itu, metode manual tidak terintegrasi secara langsung dengan sistem validasi, sehingga memperlambat proses administrasi dan meningkatkan probabilitas ketidaksesuaian data. Untuk menyelesaikan masalah ini, diperlukan pengembangan sistem yang tidak hanya memungkinkan validasi keabsahan *invoice* tetapi juga memungkinkan pembuatan *invoice* berbasis sistem yang telah terintegrasi dengan kode QR untuk memudahkan proses autentikasi.

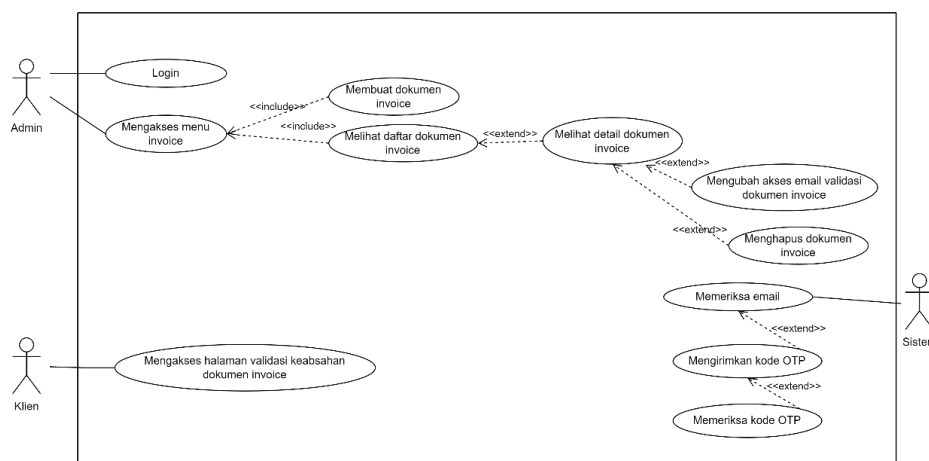
Alur proses bisnis sebelum dan sesudah adanya sistem mengalami perubahan yang signifikan, mencerminkan perbedaan dalam efisiensi dan keamanan. Perubahan ini disajikan pada Tabel 1.

Table 1 Perubahan Sebelum Dan Sesudah Implementasi Sistem

Aspek	Sebelum Implementasi Sistem	Setelah Implementasi Sistem
Pembuatan <i>Invoice</i>	Dilakukan secara manual menggunakan aplikasi <i>worksheet</i>	Diproses secara terintegrasi melalui sistem berbasis web
Validasi Keabsahan <i>Invoice</i>	Proses validasi dilakukan secara manual melalui kontak perusahaan	Proses validasi dilakukan melalui kode QR yang telah terintegrasi dengan sistem validasi keabsahan <i>invoice</i>
Keamanan Validasi	Rentan terhadap pemalsuan	Diperkuat dengan metode keamanan 2FA dilengkapi dengan penggunaan algoritma TOTP

2.3. Perancangan Sistem

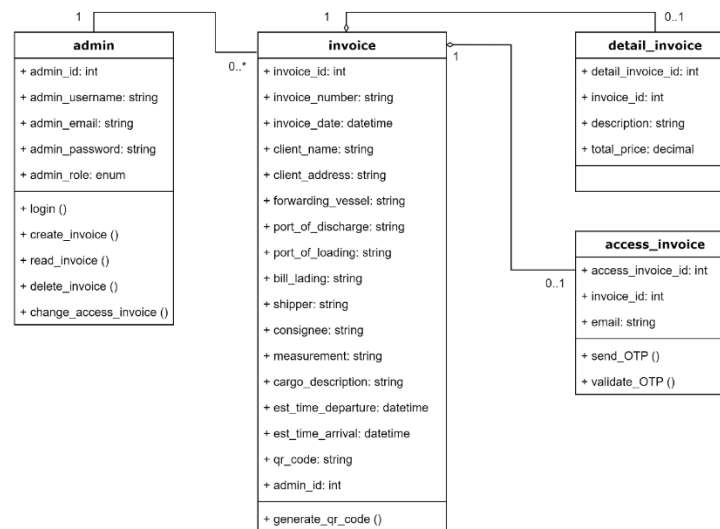
2.3.1 Use Case Diagram



Gambar 4 Use Case Diagram

Pada Gambar 4 menyajikan bagaimana istem yang dikembangkan, memiliki tiga aktor utama yaitu admin, klien, dan sistem. Aktor admin bertanggung jawab dalam pengelolaan *invoice* dan mengelola akses validasi. Aktor klien bertindak sebagai pengguna yang menerima *invoice* serta dapat melakukan proses validasi keabsahan *invoice* melalui sistem. Sedangkan, sistem bertugas memproses pengelolaan *invoice* yang diterima, memproses autentikasi yang ada serta menangani proses verifikasi dan pengiriman kode OTP.

2.3.2 Class Diagram

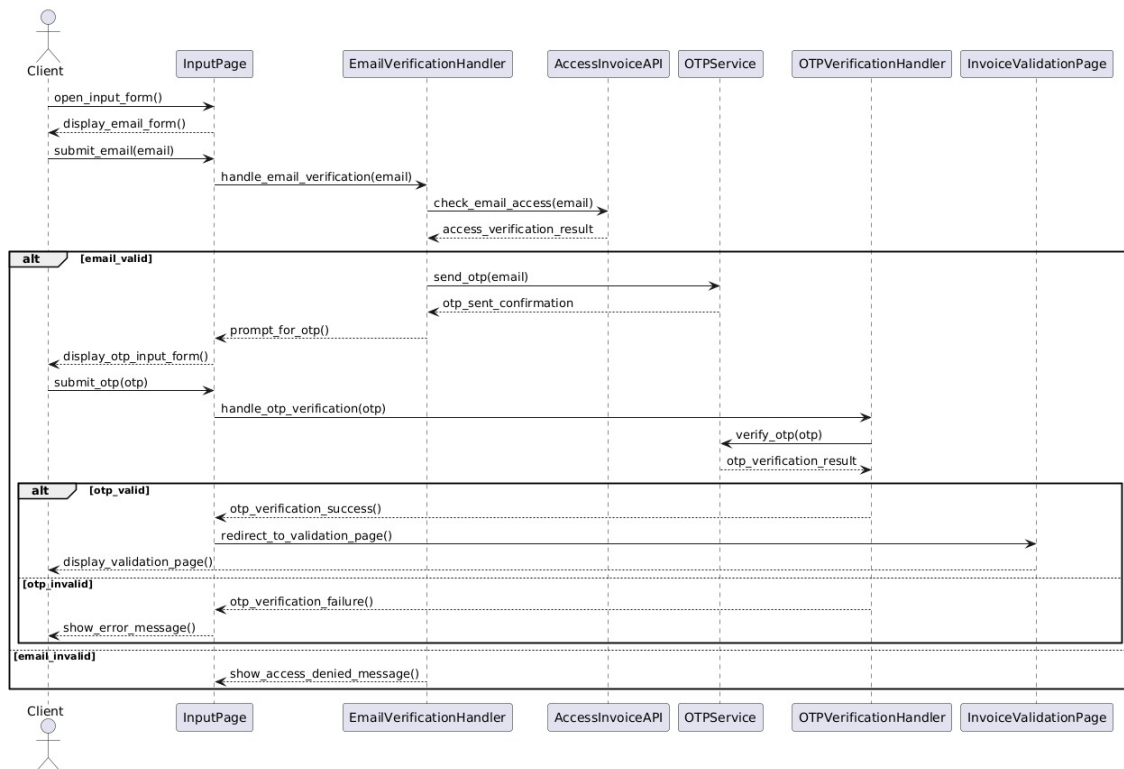


Gambar 5 Class Diagram

Pada Gambar 5 terdapat class diagram sistem yang terdiri dari empat class, yaitu *admin*, *invoice*, *detail_invoice*, dan *access_invoice*. Class *admin* memiliki beberapa metode yang dimana *admin* dapat melakukan login, mengakses menu-menu *invoice*, dan mengubah akses email *invoice*. Terdapat juga class *invoice* yang dimana memiliki metode untuk menghasilkan Kode QR untuk setiap dokumen *invoice* yang dibuat oleh *admin* nantinya. Class *detail_invoice* tersedia untuk menyimpan detail yang dimiliki oleh setiap *invoice* nantinya. Untuk class *access_invoice* ada untuk mengelola daftar email yang dapat mengakses dokumen *invoice* nantinya yang dilengkapi dengan metode pengiriman kode OTP untuk keamanan.

2.3.3 Sequence Diagram

Pada Gambar 6 menggambarkan proses yang dimulai ketika klien membuka formulir input email. Setelah mengisi email, pengguna mengirimkan data tersebut ke sistem. Sistem kemudian menerima data email dan meneruskannya ke komponen yang bertugas menangani verifikasi email yaitu *EmailVerificationHandler*. *EmailVerificationHandler* akan memeriksa apakah email yang dimasukkan oleh pengguna sudah terdaftar dan memiliki akses. Jika email valid, sistem akan mengirimkan OTP ke email pengguna melalui layanan pengiriman OTP yaitu *OTPService*. Pengguna kemudian diminta untuk memasukkan OTP yang telah dikirimkan. Setelah pengguna memasukkan OTP, sistem akan memverifikasi OTP yang dimasukkan dengan OTP yang telah dikirimkan sebelumnya. Jika OTP valid, pengguna akan diarahkan ke halaman validasi *invoice* yaitu *InvoiceValidationPage*. Namun, jika OTP tidak valid atau email tidak terdaftar, sistem akan menampilkan pesan kesalahan kepada pengguna.



Gambar 6 Sequence Diagram Proses Validasi Keabsahan Invoice

3. HASIL DAN PEMBAHASAN

3.1. Implementasi Sistem Create Invoice

Sistem ini memiliki fitur login yang terbagi menjadi dua jenis pengguna, yaitu super admin dan admin. Hak akses terhadap menu di dalam sistem akan dibatasi berdasarkan peran masing-masing pengguna. Setiap pengguna yang berhasil login dapat mengakses menu create invoice seperti yang disajikan pada Gambar 7.

The screenshot shows a web application interface for creating an invoice. The left sidebar contains a navigation menu with options: Home, Dashboard, Create Invoice (highlighted), List Invoice, Change My Password, and Logout. The main content area is titled 'Create' and includes several form sections: 'Invoice Detail' with fields for Invoice Date, Client Name, Client Address, Forwarding Name, Port of Discharge, Port of Loading, and Bill Loading; 'Shipper' and 'Consignee' fields; 'Measurement' and 'Cargo Description' fields; 'Estimated Time Departure' and 'Estimated Time Arrival' fields. Below these are sections for 'Charge Description' and 'Access Email', each with a table for adding items. The bottom of the page has a 'Save Invoice' button.

Gambar 7 Halaman Create Invoice

PT. MANDIRI BERSAMA
cargo service

Jl. Sanggar No 31-33
Surabaya (60175)
Telp. : +6231-73690229
Fax. : +6231-3576864
INDONESIA

Invoice

Bill To:
COCONUT JAYA SENTOSA
MADURA, INDONESIA

Invoice Number: 082/C/S/02030210
Date: 10-02-2025
Terms: CASH ONLY

Forwarding Vessel: STARSHIP NEPTUNE V.2405N
Port Of Discharge: QINGDAO, CHINA
Part Of Loading: SURABAYA, INDONESIA
Bill Lading: 44310006332
Shipper: COCONUT JAYA SENTOSA
Consignee: CHINA NATIONAL TOWNSHIP ENTERPRISES CO.,LTD
Measurement: 468 PACKAGES
Cargo Description: COCONUT FIBER
ETD/ETA: 13-02-2025 / 13-03-2025

Charge Description	Amount
SEA FREIGHT	IDR 13,500,000
TELEX BL	IDR 1,100,000
Total Amount:	IDR 14,600,000

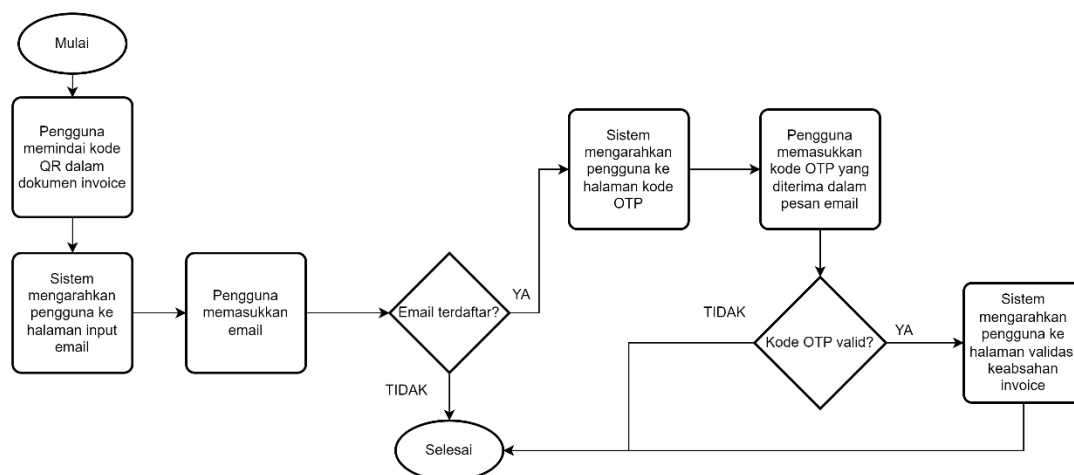
PAYMENT SHOULD BE RECEIVED IN FULL AMOUNT
PT. MANDIRI BERSAMA
IDR REK No: 1400012290296
BANK MANDIRI Ctb. Surabaya Niaga

*Scan the QR code to validate invoice authenticity

Gambar 8 Dokumen Invoice Dengan Integrasi Kode QR

Gambar 8 menampilkan dokumen *invoice* yang dihasilkan oleh sistem dari data *invoice* yang telah diinputkan pengguna melalui form create *invoice* pada Gambar 7. Kode QR digunakan dalam dokumen *invoice* guna menjadi media yang dapat menghubungkan pengguna dengan sistem validasi keabsahan *invoice*. Selain bentuknya yang cukup praktis untuk dilampirkan pada sebuah dokumen yang memiliki keterbatasan ruang, kode QR juga mampu menyimpan berbagai macam informasi di dalamnya. Dengan itu, kode QR dapat menyimpan tautan unik untuk setiap *invoice*-nya yang dapat digunakan untuk memvalidasi keabsahan dokumen *invoice* tersebut. Selain itu, kode QR juga dapat dipindai dengan mudah menggunakan berbagai perangkat, misalnya *smartphone*. Sehingga, mempercepat proses validasi keabsahan *invoice* tanpa membutuhkan proses secara manual lagi.

3.2. Implementasi 2FA dan Algoritma TOTP



Gambar 9 Alur Proses Validasi Keabsahan Invoice

Pada Gambar 9, sistem mulai memproses permintaan validasi keabsahan *invoice* setelah pengguna memindai kode QR dalam dokumen *invoice* dan dilanjutkan sistem menampilkan

halaman input email, yang dimana email merupakan langkah pertama dalam metode keamanan 2FA yang diterapkan dalam sistem. Setelah pengguna memasukkan email, sistem akan memeriksa apakah email tersebut valid. Jika valid, sistem akan mengarahkan pengguna ke halaman input kode OTP.

Kode OTP ini berperan sebagai langkah kedua dalam metode keamanan 2FA yang diterapkan dalam sistem. Selain mengarahkan pengguna ke halaman input kode OTP, sistem juga akan mengirimkan kode OTP ke email tersebut, yang dimana kode OTP tersebut dihasilkan dari algoritma TOTP yang digunakan dalam sistem dengan memanfaatkan *secret key* dan *time* sebagai counter-nya. Setelah pengguna memasukkan kode OTP yang diterima, sistem akan memeriksa apakah kode OTP tersebut valid. Jika valid, sistem akan mengarahkan pengguna ke halaman yang menampilkan informasi terkait keabsahan invoice tersebut.

Penerapan algoritma TOTP dalam sistem (seperti pada Tabel 2), algoritma TOTP bergantung pada dua parameter utama, yaitu *secret key* dan *time* sebagai counter-nya. Fungsi *generateTOTP* digunakan untuk menghasilkan kode OTP. Prosesnya dimulai dengan menghitung waktu saat ini dalam format UNIX timestamp dan membaginya dengan interval waktu (step) yang telah ditentukan untuk mendapatkan time counter. Counter ini kemudian dikonversi menjadi buffer 8-byte dalam format big-endian, yang akan digunakan sebagai input untuk perhitungan TOTP. Selanjutnya, sistem menerapkan algoritma HMAC-SHA1, di mana secret key dan time counter digunakan sebagai parameter untuk menghasilkan kode hash. Setelah kode hash diperoleh, sistem melakukan dynamic truncation dengan mengambil beberapa bagian byte dari hasil kode hash. Nilai yang diperoleh dari proses dynamic truncation dikonversi menjadi bilangan bulat positif, kemudian dilakukan operasi modulus untuk memastikan bahwa kode OTP yang dihasilkan hanya terdiri dari 6 digit numerik. Fungsi ini akhirnya mengembalikan kode OTP dengan panjang yang telah ditentukan.

Table 2 Kode Program Algoritma TOTP

```

1. import crypto from 'crypto';
2. function hmacSha1(key, message) {
3.   const hmac = crypto.createHmac('sha1', key);
4.   hmac.update(message);
5.   return hmac.digest('hex');
6. }
7. function dynamicTruncation(hmacHash) {
8.   const offset = parseInt(hmacHash.slice(-1), 16);
9.   const binary = parseInt(hmacHash.substr(offset * 2, 8), 16);
10.  return binary & 0x7fffffff;
11. }
12. export function generateTOTP(secret, step = 60, digits = 6, offset = 0) {
13.   const timestamp = Math.floor(Date.now() / 1000);
14.   let counter = Math.floor(timestamp / step) + offset;
15.   const message = Buffer.alloc(8);
16.   for (let i = 7; i >= 0; i--) {
17.     message[i] = counter & 0xff;
18.     counter >>= 8;
19.   }
20.   const hmacHash = hmacSha1(secret, message);
21.   const truncated = dynamicTruncation(hmacHash);
22.   const otp = truncated % Math.pow(10, digits);
23.   return otp.toString().padStart(digits, '0');
24. }
25. export function verifyTOTP(secret, userOtp, step = 60, digits = 6) {
26.   const currentOtp = generateTOTP(secret, step, digits, 0);
27.   const previousOtp = generateTOTP(secret, step, digits, -1);
28.   return userOtp === currentOtp || userOtp === previousOtp;
29. }

```

Sementara itu, fungsi verifyTOTP digunakan untuk memverifikasi kode OTP yang dimasukkan oleh pengguna. Proses ini dilakukan dengan menghasilkan kode OTP saat ini menggunakan generateTOTP dan membandingkannya dengan kode OTP yang dimasukkan oleh pengguna. Jika kode yang dimasukkan pengguna sesuai dengan OTP saat ini atau satu periode sebelumnya, maka sistem akan menganggap OTP valid dan memberikan akses ke pengguna. Dengan pendekatan ini, sistem tetap aman karena hanya menerima kode OTP yang masih berada dalam rentang waktu yang valid, sekaligus memberikan toleransi terhadap perbedaan waktu dalam proses validasi keabsahan *invoice*.

3.3. Proses Validasi Keabsahan Invoice

Proses validasi keabsahan invoice dimulai dengan memindai kode QR dalam dokumen invoice (seperti pada Gambar 10) yang dibuat menggunakan sistem. Kode QR dalam dokumen invoice menyimpan informasi berupa tautan unik yang mengarahkan ke status validasi dokumen invoice tersebut. Tautan unik tersebut telah diperkuat keamanannya dengan menggunakan *UUID* (*Universally Unique Identifier*). *UUID* dipilih karena memiliki struktur yang kompleks dan acak, sehingga sulit ditebak dibandingkan ID numerik yang rentan terhadap *enumeration attack*. Selain itu, *UUID* membantu mencegah manipulasi data dengan mengurangi kemungkinan pengguna mencoba mengakses invoice lain hanya dengan mengganti tautan.

Dengan memanfaatkan metode keamanan 2FA menggunakan email dan kode OTP, sistem juga dilengkapi dengan pengecekan alamat email, yang dimana jika alamat email tidak terdaftar dalam sistem, maka sistem tidak akan mengirimkan pesan email berisikan kode OTP ke email tersebut dan tidak akan mengarahkan pengguna ke halaman memasukkan kode OTP. Selain itu, sistem juga dilengkapi dengan mekanisme *rate limiting* pada verifikasi kode OTP untuk mencegah *brute force attack*. Jika pengguna, salah memasukkan kode OTP sebanyak tiga kali, maka proses validasi akan dikunci sementara selama sepuluh menit.

CV. MANDIRI BERSAMA
cargo service

Jl. Sanggar No 31-33
Surabaya (60175)
Telp. : +6231-73890229
Fax. : +6231-3576884
INDONESIA

Invoice

Bill To:
MR. KRISNO
SURABAYA

Invoice Number: 095/MK/20170105
Date: 05-01-2017
Terms: CASH ONLY

Forwarding Vessel: NORTHERN DECISION V.152QAN
Port Of Discharge: PROVIDENCIALES TC
Port Of Loading: SURABAYA, INDONESIA
Bill Lading: DJA0346609
Shipper: CV. CIPTA KARYA
Consignee: OLIVER STUBBS / ODDS & ENDS
Measurement: 12 PALLETS = 13,751 PCS = 19,5293 M3
Cargo Description: INDONESIAN WOOD WORKING PRODUCTS
ETD/ETA: 19-02-2025 / 19-03-2025

Charge Description	Amount
SEA FREIGHT	IDR 70,460,200
INSURANCE	IDR 1,345,000

Total Amount: IDR 71,805,200

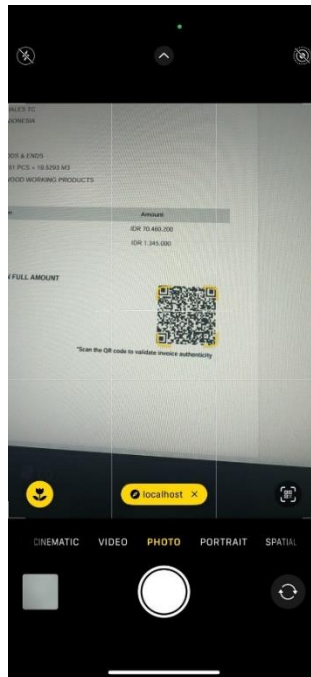
PAYMENT SHOULD BE RECEIVED IN FULL AMOUNT
CV. MANDIRI BERSAMA
IDR REK No: 1400012299286
BANK MANDIRI Cab. Surabaya Niaga.

Scan the QR code to validate invoice authenticity

Gambar 10 Dokumen Invoice

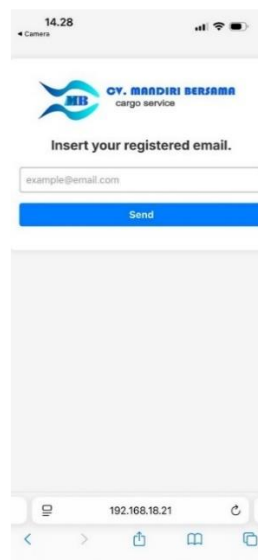
Setelah membuka dokumen *invoice* yang diterima, jika ingin memvalidasi keabsahan *invoice*, maka dapat memindai kode QR yang tersedia pada dokumen *invoice* dengan menggunakan perangkat yang dimiliki. *Smartphone* merupakan perangkat yang dapat digunakan

untuk memindai kode QR dan mengakses informasi yang ada didalamnya seperti pada Gambar 11.



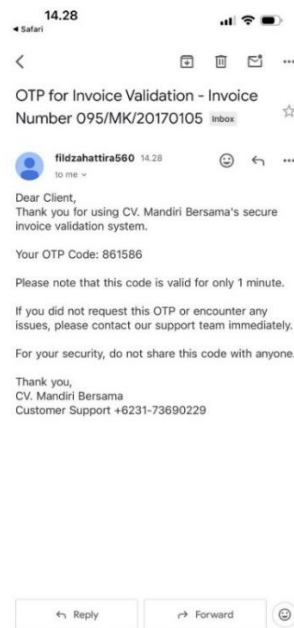
Gambar 11 Memindai Kode QR Dengan Smartphone

Saat telah berhasil memindai kode QR, dilanjutkan dengan mengakses informasi yang tersimpan di dalamnya. Dalam proses validasi keabsahan invoice ini, informasi yang tersimpan dalam kode QR yaitu berupa tautan unik pada setiap dokumen *invoice*-nya yang akan mengarahkan pengguna ke halaman untuk memasukkan email yang telah terdaftar dalam sistem dan memiliki akses untuk melihat keaslian dokumen invoice tersebut. Halaman untuk memasukkan alamat email tersedia pada Gambar 12.

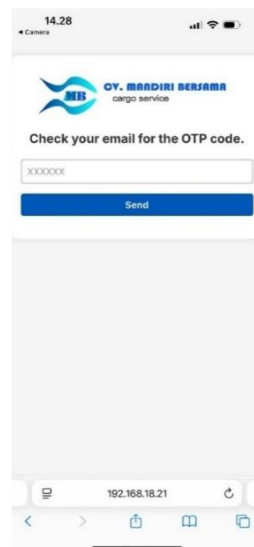


Gambar 12 Halaman Memasukkan Email

Setelah pengguna memasukkan alamat email, maka akan dilakukan pengecekan oleh sistem. Jika alamat email tersebut memiliki akses, maka sistem akan mengirimkan pesan berisikan kode OTP ke alamat email tersebut. Pesan kode OTP tersedia pada Gambar 13.

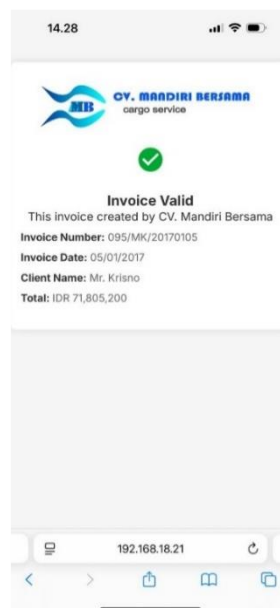


Gambar 13 Pesan Berisikan Kode OTP



Gambar 14 Halaman Memasukkan Kode OTP

Selain mengirimkan pesan berisikan kode OTP, sistem juga akan mengarahkan pengguna yang memiliki akses ke halaman untuk memasukkan kode OTP yang didapatkan. Halaman memasukkan kode OTP tersedia pada Gambar 14. Setelah pengguna memasukkan kode OTP dan kode tersebut dianggap valid oleh sistem, maka sistem akan mengarahkan pengguna ke halaman yang menyajikan informasi keabsahan dokumen *invoice* tersebut seperti yang tersedia pada Gambar 4.31.



Gambar 15 Halaman Validasi Keabsahan Invoice

4. KESIMPULAN

Sistem ini telah berhasil dikembangkan untuk mendukung proses bisnis pada CV. Mandiri Bersama menggunakan framework Next.js. Proses pengembangan mencakup beberapa tahapan, yaitu identifikasi masalah, analisis kebutuhan, studi literatur, perancangan sistem, pengembangan sistem, hingga pengujian dengan metode black-box testing. Sistem ini menerapkan QR Code sebagai metode validasi keabsahan invoice, di mana setiap invoice yang dihasilkan memiliki QR Code unik. Ketika QR Code dipindai, pengguna harus memasukkan email yang terdaftar untuk menerima kode OTP yang dihasilkan menggunakan algoritma Time-based One-Time Password (TOTP). OTP dikirimkan melalui email, bersifat sementara, dan hanya dapat digunakan dalam jangka waktu tertentu.

Dengan penerapan metode keamanan Two-Factor Authentication (2FA) berbasis email dan OTP, sistem ini memastikan bahwa hanya pengguna dengan email yang memiliki akses terdaftar yang dapat melakukan validasi, sehingga mengurangi risiko penyalahgunaan atau pemalsuan invoice oleh pihak yang tidak berwenang. Berdasarkan hasil pengujian, implementasi QR Code dan algoritma TOTP dalam sistem validasi keabsahan invoice berjalan efektif sesuai dengan proses bisnis CV. Mandiri Bersama. Sistem ini mampu memastikan bahwa hanya pengguna dengan akses terdaftar yang dapat melakukan validasi invoice. Efektivitas ini dicapai melalui mekanisme validasi yang menggunakan QR Code unik untuk mengarahkan pengguna ke sistem resmi, serta penerapan Two-Factor Authentication (2FA) berbasis email dan OTP yang bersifat sementara. Selain itu, halaman validasi hanya dapat diakses setelah melewati proses 2FA, sehingga mencegah pihak yang tidak berwenang membuat tiruan website untuk manipulasi. Dengan demikian, sistem ini tidak hanya melindungi keabsahan invoice tetapi juga mengurangi risiko phishing atau upaya pemalsuan situs validasi.

5. SARAN

Sebagai langkah pengembangan lebih lanjut, sistem ini dapat dioptimalkan dengan menerapkan notifikasi otomatis kepada pengguna terkait status invoice. Notifikasi ini dapat memberikan informasi real-time mengenai perubahan status invoice, seperti pembuatan, persetujuan, atau pembayaran yang telah dilakukan. Selain itu, integrasi dengan layanan pembayaran digital dapat meningkatkan efisiensi dan kemudahan dalam proses transaksi, memungkinkan pengguna untuk langsung menyelesaikan pembayaran melalui sistem.

DAFTAR PUSTAKA

- [1] Lorien, A., & Wellem, T. (2021). Implementasi Sistem Otentikasi Dokumen Berbasis Quick Response (QR) Code dan Digital Signature. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, 5(4), 663-671.
- [2] Husna, L., & Rizki, S. N. (2023). Pemanfaatan JST Pengenalan Keaslian Pola Tanda Tangan untuk Pencegahan Tindakan Pemalsuan Tanda Tangan. *Jurnal Teknik Informatika UNIKA Santo Thomas*, 116-124.
- [3] Sukabumi, A. G. A. B. (2016). Penggunaan QR code sarana penyampaian promosi dan informasi kebun binatang berbasis android. *Bianglala Informatika*, 4(1).
- [4] Idrus, S. Z. S., Cherrier, E., Rosenberger, C., & Schwartzmann, J. J. (2013). A review on authentication methods. *Australian Journal of Basic and Applied Sciences*, 7(5), 95-107.
- [5] Setiawan, H., Sartika, D., & Ramadhan, B. G. (2020). Implementasi Time-Based One Time Password (TOTP) Pada Sistem Two Factor Authentication (2FA). *Jurnal Teknologi*, 13(1), 63-68.
- [6] Qadriah, L., & Achmady, S. (2023). Sistem Pengamanan Dokumen dengan Algoritma Time-Based One Time Password (TOTP) pada Two-Factor Authentation (2FA). *Jurnal Sains dan Informatika*, 29-35.
- [7] Sari, A. N., & Abdillah, T. G. (2021). Metode Absensi Mahasiswa berbasis QR Code dan Time-Based One-Time Password. *Jurnal Informatika Polinema*, 7(2), 29-34. <https://doi.org/10.33795/jip.v7i2.492>
- [8] Qadriah, L., Achmady, S., & Husaini. (2023). Sistem Pengamanan Dokumen dengan Algoritma Time-Based One Time Password (TOTP) pada Two-Factor Authentication (2FA). *Jurnal Sains dan Informatika*, 9(1), 29-35. <https://doi.org/10.34128/jsi.v9i1.519>.
- [9] Wibawa, S., Suryanto, & Ningsih, R. (2024). Perlindungan Data Digital Dengan Time-Based One-Time Password (TOTP). *INSANtek*, 5(1), 30-36. <https://doi.org/10.31294/insantek.v5i1.3495>.
- [10] Hayat, M. A. M., Abbas, R., & Bakti, R. Y. (2022). Desain dan Implementasi Time Based One Time Password untuk Meningkatkan Keamanan Otentikasi pada Website Top Up Gaming. *Ainet: Jurnal Informatika*, 4(1), 16-23. <https://doi.org/10.26618/ainet.v4i1.8897>.
- [11] Putri, T. D., Sugeng, W., & Utama, G. Y. (2020). Tempat Sampah Pengelola Password Wifi dengan Algoritma TOTP SHA-3. *MIND (Multimedia Artificial Intelligent Networking Database) Journal*, 5(1).
- [12] Junaidi, A., Wibowo, G. W. N., Sucipto, A., & Zyen, A. K. (2026). Penyedia Pengamanan Login pada Sistem Informasi Menggunakan Timed Based One Time Password. *JTINFO: Jurnal Teknik Informatika*, 5(1), 381-390. <https://doi.org/10.02220/jtinfo.v5i1.1886>.
- [13] Yahya, A., Kusyanti, A., & Trisnawan, P. H. (2025). Implementasi Time-Based One-Time Password Menggunakan Algoritma Photon untuk Autentikasi Dua Faktor. *Jurnal Teknologi Informasi dan Ilmu Komputer*, 12(4), 799-808.

- [14] Ungkawa, U., & Putra, K. R. (2017). Implementasi Algoritma Time-Based One Time Password dalam Otentikasi Token Internet Banking. Project Report, LPPM ITENAS.
- [15] Herri, S., Dewi, S., & Boy, G. R. (2020). Implementasi Time-Based One Time Password (TOTP) pada Sistem Two Factor Authentication (2FA). Jurnal Teknologi, 13(1), 63–?
- [16] Hapsari, N. S., Fatman, Y., & Isbandi. (2020). Implementasi Metode One Time Password pada Sistem Pemesanan Online. Jurnal Media Informatika Budidarma, 4(4), 930–939. <https://doi.org/10.30865/mib.v4i4.2195>