

**PENERAPAN TWO-FACTOR AUTHENTICATION (2FA) DENGAN  
MENGUNAKAN  
METODE TIME-BASED ONE-TIME PASSWORD (TOTP) REAL-TIME  
DATABASE DI  
KEDAI SAMPAN TRADISIONAL SAMARINDA**

**SKRIPSI**

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana  
Program Studi Informatika



disusun oleh

**ICHWANUTAKWA BAGASKARA**

**22.21.1549**

Kepada

**FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA**

**2022**

**PENERAPAN TWO-FACTOR AUTHENTICATION (2FA) DENGAN  
MENGUNAKAN  
METODE TIME-BASED ONE-TIME PASSWORD (TOTP) REAL-TIME  
DATABASE DI  
KEDAI SAMPAN TRADISIONAL SAMARINDA**

**SKRIPSI**

untuk memenuhi salah satu syarat mencapai derajat Sarjana  
Program Studi Informatika



disusun oleh

**ICHWANUTAKWA BAGASKARA**

**22.21.1549**

Kepada

**FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA**

**2022**



**HALAMAN PERSETUJUAN**

**SKRIPSI**

**PENERAPAN TWO-FACTOR AUTHENTICATION (2FA) DENGAN  
MENGUNAKAN  
METODE TIME-BASED ONE-TIME PASSWORD (TOTP) REAL-TIME  
DATABASE DI  
KEDAI SAMPAN TRADISIONAL SAMARINDA**

yang disusun dan diajukan oleh

**Ichwanutakwa Bagaskara**

**22.21.1549**

telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal 25/07/2024

Dosen Pembimbing,



**Kusnawi, S.Kom, M.Eng.**

**NIK. 190302112**



**HALAMAN PENGESAHAN**

**SKRIPSI**

**PENERAPAN TWO-FACTOR AUTHENTICATION (2FA) DENGAN  
MENGUNAKAN  
METODE TIME-BASED ONE-TIME PASSWORD (TOTP) REAL-TIME  
DATABASE DI  
KEDAI SAMPAN TRADISIONAL SAMARINDA**

yang disusun dan diajukan oleh

**Ichwanutakwa Bagaskara**

**22.21.1549**

Telah dipertahankan di depan Dewan Penguji  
pada tanggal 25/07/2024

**Susunan Dewan Penguji**

**Nama Penguji**

**Tanda Tangan**

**Bayu Setiaji, M.Kom**  
NIK. 190302216

**Dina Maulina, S.Kom., M.Kom**  
NIK. 190302250

**Kusnawi, S.Kom, M.Eng.**  
NIK. 190302112



Skripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
Tanggal 25/07/2024

**DEKAN FAKULTAS ILMU KOMPUTER**



**Hanif Al Fatta, S.Kom., M.Kom., Ph.D.**  
NIK. 190302096



## HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Ichwanutakwa Bagaskara  
NIM : 22.21.1549

Menyatakan bahwa Skripsi dengan judul berikut:

**Penerapan Two-Factor Authentication (2FA) Dengan Menggunakan Metode Time-Based One-Time Password (TOTP) Real-Time Database Di Kedai Sampan Tradisional Samarinda**

Dosen Pembimbing : Kusnawi, S.Kom, M. Eng

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 25 Juni 2024

Yang Menyatakan,



Ichwanutakwa Bagaskara

## HALAMAN PERSEMBAHAN

Skripsi ini saya persembahkan untuk:

1. Kedua orang tua saya, Bapak Zulkarnain dan Ibu Novarina Lukitaningsih, yang telah memberikan dukungan, doa, dan kasih sayang yang tiada henti. Terima kasih atas segala pengorbanan, didikan, dan perjuangan kalian dalam membesarkan dan mendidik saya hingga saat ini.
2. Dosen pembimbing saya, Bapak Kusnawi, S.Kom, M. Eng, yang dengan sabar dan tulus membimbing serta mengarahkan saya hingga skripsi ini dapat terselesaikan dengan baik.
3. Seluruh dosen dan staf pengajar di Fakultas Ilmu Komputer/S1-Informatika yang telah memberikan ilmu, motivasi, dan bantuan selama saya menempuh pendidikan di universitas ini.
4. Teman-teman seperjuangan di Fakultas Ilmu Komputer/S1-Informatika angkatan 2022 Transfer, yang telah berjuang bersama-sama, saling mendukung, dan berbagi canda tawa selama masa perkuliahan.
5. Semua pihak yang tidak dapat saya sebutkan satu per satu, yang telah membantu dan mendukung saya dalam menyelesaikan studi ini.

Semoga skripsi ini dapat bermanfaat dan menjadi sumbangan pemikiran bagi pengembangan ilmu pengetahuan. Terima kasih atas segala dukungan dan doa yang telah diberikan.

## KATA PENGANTAR

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa atas segala rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan skripsi ini dengan baik. Skripsi yang berjudul "Penerapan Two-Factor Authentication (2FA) Dengan Menggunakan Metode Time-Based One-Time Password(TOTP) Real-Time Database di Kedai Sampan Tradisional Samarinda" ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana di Universitas AMIKOM Yogyakarta. Penyusunan skripsi ini tidak terlepas dari bantuan, bimbingan, dan dukungan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis ingin menyampaikan ucapan terima kasih kepada:

1. Bapak/Ibu Hanif Al Fatta, S.Kom., M.Kom., Ph.D, selaku Dekan Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta
2. Bapak/Ibu Windha Mega Pradnya Duhita, M.kom, selaku Ketua Program Studi S1-Informatika.
3. Bapak/Ibu Kusnawi, S.Kom, M. Eng, selaku Dosen Pembimbing yang telah meluangkan waktu, tenaga, dan pemikirannya untuk membimbing dan mengarahkan penulis dalam menyelesaikan skripsi ini.
4. Seluruh Dosen dan Staf Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta yang telah memberikan ilmu pengetahuan, bimbingan, dan bantuan selama penulis menempuh pendidikan.
5. Keluarga tercinta, Ayah, Ibu, dan saudara-saudara, atas doa, dukungan, dan motivasi yang tiada henti diberikan kepada penulis.

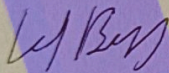


6. Teman-teman S1-Informatika angkatan 2022 Transfer, atas segala bantuan, semangat, dan kerja sama yang telah diberikan.
7. Semua pihak yang telah membantu dalam penyelesaian skripsi ini yang tidak dapat penulis sebutkan satu per satu.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Oleh karena itu, penulis mengharapkan kritik dan saran yang membangun dari pembaca. Semoga skripsi ini dapat bermanfaat bagi penulis khususnya dan bagi pembaca pada umumnya.

Yogyakarta, 9 Juni 2024

Penulis



Ichwanutakwa Bagaskara



## DAFTAR ISI

HALAMAN JUDUL .....	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN .....	iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI .....	iv
HALAMAN PERSEMBAHAN .....	v
KATA PENGANTAR .....	vi
DAFTAR ISI.....	viii
DAFTAR TABEL.....	xi
DAFTAR GAMBAR .....	xii
DAFTAR LAMPIRAN.....	xiii
DAFTAR ISTILAH .....	xiv
INTISARI .....	xv
<i>ABSTRACT</i> .....	xvi
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	2
1.3 Batasan Masalah.....	2
1.4 Tujuan Penelitian.....	2
1.5 Manfaat Penelitian.....	3
1.6 Sistematika Penulisan.....	3
BAB II TINJAUAN PUSTAKA .....	5
2.1 Studi Literatur .....	5

2.2	Dasar Teori .....	7
2.2.1	<i>Two-Factor authentication (2FA)</i> .....	7
2.2.2	<i>One-Time Password (OTP) dan Time-Based One-Time Password (TOTP)</i> .....	7
2.2.3	Laravel .....	8
2.2.4	Sistem Informasi .....	9
2.2.5	PHP .....	9
2.2.6	Framework .....	9
2.2.7	Bootstrap .....	10
2.2.8	Restoran .....	10
2.2.9	Google Authenticator .....	11
2.2.10	Database .....	12
2.2.11	Metode Waterfall .....	13
2.2.12	UML .....	14
2.2.13	Firebase .....	20
<b>BAB III METODE PENELITIAN .....</b>		<b>21</b>
3.1	Objek Penelitian .....	21
3.2	Alur Penelitian .....	21
3.3	Alat dan Bahan .....	23
3.4	Rancangan Penelitian .....	24
3.4.1	Perancangan UML .....	24
3.4.2	Perancangan Database .....	27
3.4.3	Perancangan Tampilan .....	28
3.4.4	Perancangan Pengujian .....	31
3.4.5	Perancangan Alur Sistem .....	32





BAB IV HASIL DAN PEMBAHASAN .....	35
4.1 Implementasi Sistem .....	35
4.1.1 Deskripsi Sistem .....	35
4.1.2 Tampilan Antar Muka Sistem .....	35
4.1.3 Tampilan Antar Muka User .....	36
4.1.4 Tampilan Antar Muka Admin .....	38
4.2 Uji Sistem .....	39
4.2.1 <i>BlackBox Testing</i> .....	39
4.2.2 <i>WhiteBox Testing</i> .....	41
4.3 Mekanisme Aplikasi .....	44
BAB V PENUTUP .....	45
5.1 Kesimpulan .....	45
5.2 Saran .....	45
REFERENSI .....	47
LAMPIRAN .....	50

## DAFTAR TABEL

Tabel 2.1. Keaslian Penelitian	8
Tabel 2.2. Simbol – Simbol <i>Use Case</i> Diagram	15
Tabel 2.3. Simbol – Simbol <i>Activity</i> Diagram	16
Tabel 2.4. Simbol – Simbol <i>Sequences</i> Diagram	17
Tabel 2.5. Simbol – Simbol <i>Class</i> Diagram	19
Tabel 3.1. Pengujian Black Box	31
Tabel 4.1. Tabel BlackBox Testing	39



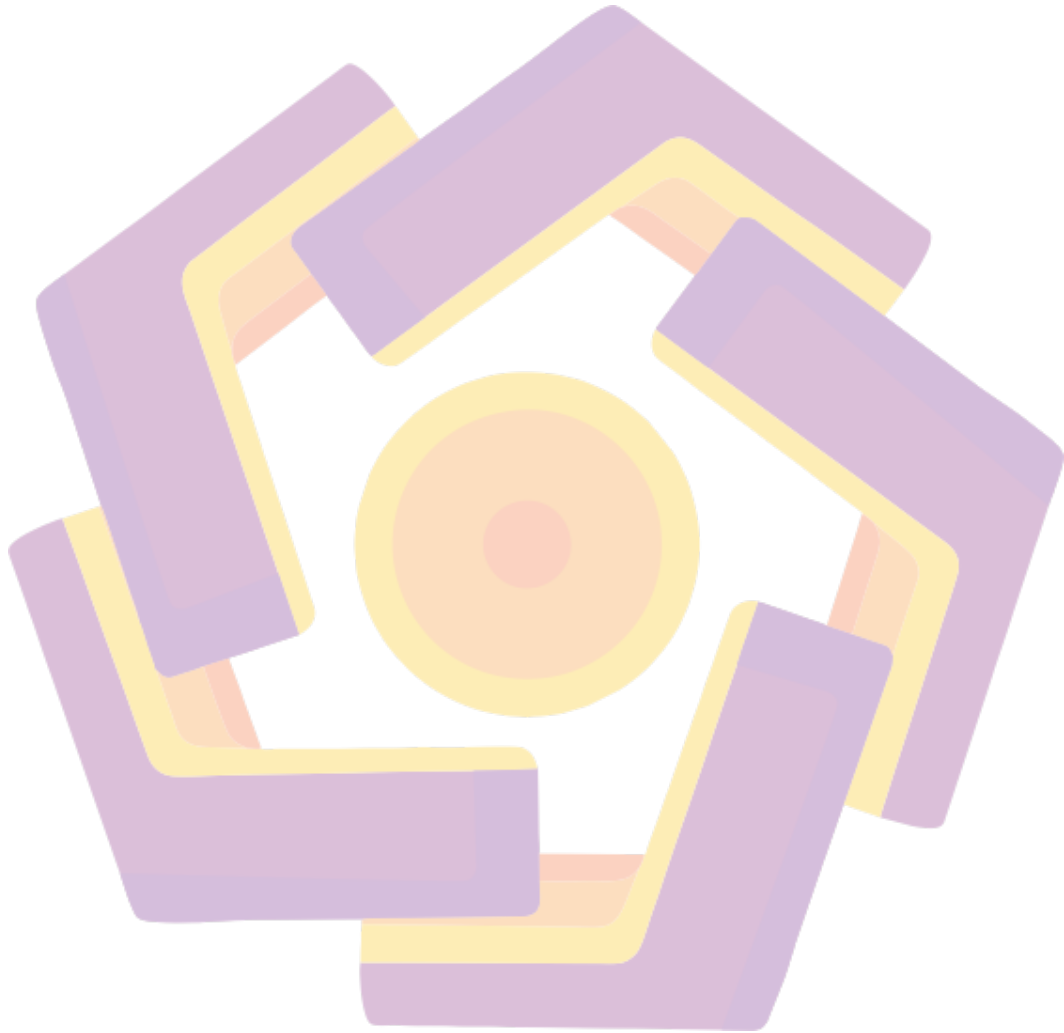


## DAFTAR GAMBAR

Gambar 2.1. Fase – Fase Metode Waterfall	14
Gambar 2.2. Contoh Use Case Diagram	16
Gambar 2.3. Contoh Activity Diagram	17
Gambar 2.4. Contoh Sequence Diagram	18
Gambar 2.5. Contoh Class Diagram	19
Gambar 2.6. Arsitektur Sistem Firebase	20
Gambar 3.1. Alur Penelitian	22
Gambar 3.2. Use Case Diagram	24
Gambar 3.3. Sequence Diagram	25
Gambar 3.4. Class Diagram	26
Gambar 3.5. Activity Diagram	27
Gambar 3.6. Desain Database	28
Gambar 3.7. Login Admin	29
Gambar 3.8. Halaman Authentication	30
Gambar 3.9. Kode TOTP	30
Gambar 3.10. Halaman Admin	31
Gambar 3.11. Alur Sistem Reservasi	34
Gambar 4.1. Tampilan Halaman Login	35
Gambar 4.2. Tampilan Halaman Register	36
Gambar 4.3. Tampilan Halaman User	36
Gambar 4.4. Tampilan Scan QR atau Secret Key	37
Gambar 4.5. Tampilan Verifikasi Kode TOTP	37
Gambar 4.6. Tampilan Halaman User	38
Gambar 4.7. Tampilan Halaman Orderan/Pembelian	38
Gambar 4.8. Tampilan Halaman Menu	39
Gambar 4.9. Tampilan Halaman Log	39
Gambar 4.10. Flow Graph White Box Testing	42

## DAFTAR LAMPIRAN

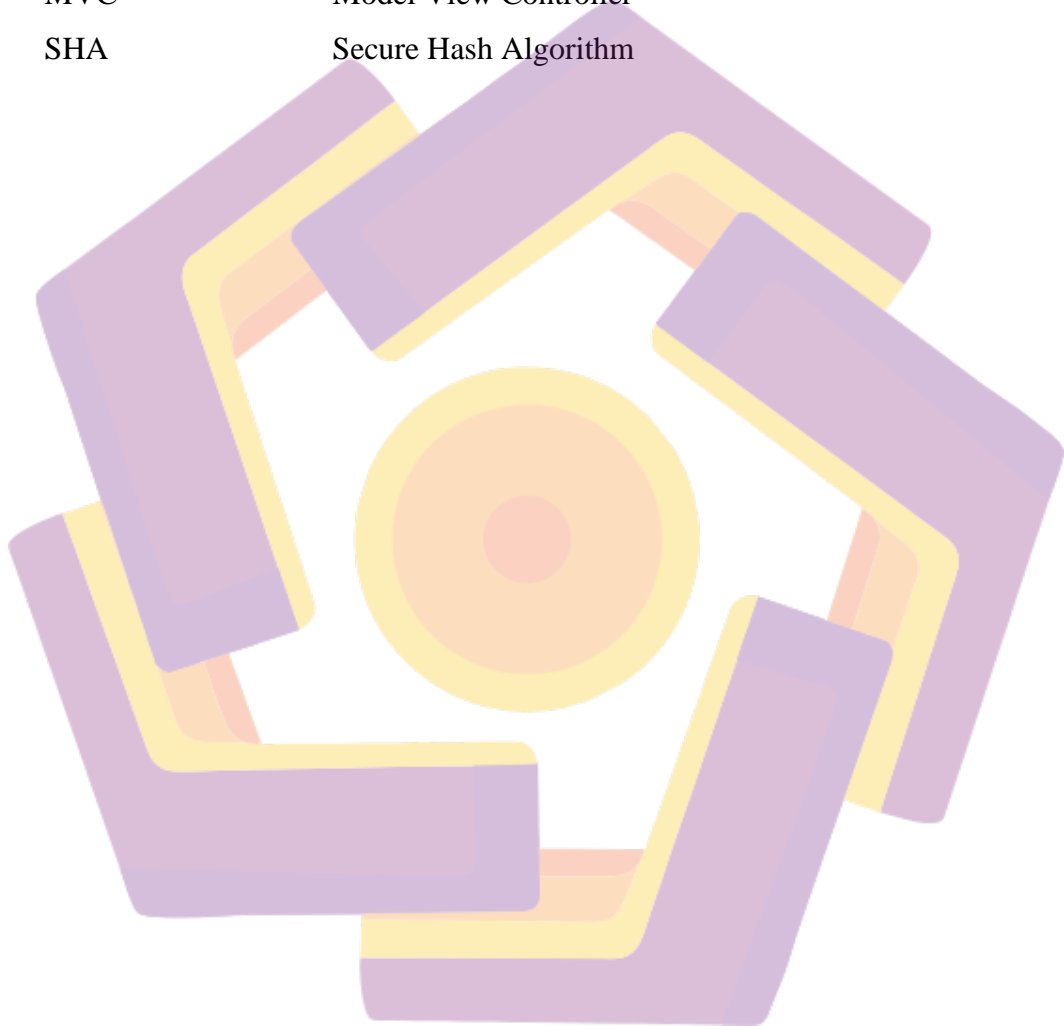
Lampiran 1. Surat Izin Penelitian





## DAFTAR ISTILAH

2FA	Two – Factor Authentication
TOTP	Time-Based One-Time Password
OTP	One-Time Password
MVC	Model View Controller
SHA	Secure Hash Algorithm



## INTISARI

Keamanan jaringan adalah tindakan yang terlibat dalam mendeteksi dan mencegah tindakan jahat. Keamanan jaringan komputer memerlukan suatu sistem yang dapat memberikan peringatan dini terhadap adanya penyusupan oleh pengguna yang tidak bertanggung jawab. Demi keamanan, login ke halaman masih manual dan memakan waktu yang cukup lama. Oleh karena itu, menggunakan teknologi OTP berbasis email untuk memungkinkan pengguna masuk ke situs web Anda dengan cepat dan mudah. Sistem dibuat dengan membuka halaman administrasi website prototype yang sedang Anda buat. Pengguna memasukkan kode OTP yang dikirimkan ke email admin yang diterima dari website prototipe. Setelah pengguna memasukkan nama pengguna dan kata sandi, kode OTP akan dikirimkan ke alamat email administrator. Kode selanjutnya dimasukkan pada halaman login web prototype untuk masuk ke halaman website prototype administrator dan diproses oleh sistem untuk menentukan informasi yang dibutuhkan oleh administrator. Hasil penelitian ini menunjukkan bahwa prototipe sistem login dengan keamanan OTP berbasis website diimplementasikan sesuai dengan algoritma yang dikembangkan oleh, dan transmisi kode OTP dilakukan melalui email administrator yang mengakses portal manajemen yang disediakan bahwa ini akan dilakukan melalui email. Login Pastikan alamat email yang Anda masukkan sesuai dengan alamat email yang terdaftar di sistem database.

**Kata kunci:** Keamanan Jaringan, Login Page, Notifikasi Email,

## ***ABSTRACT***

Network security is the practice involved in detecting and preventing malicious actions. Computer network security requires a system capable of providing early warnings against intrusion by unauthorized users. For security reasons, logging into the page is still manual and time-consuming. Therefore, implementing OTP (One-Time Password) technology based on email allows users to access your website quickly and easily. The system is designed by accessing the administration page of the prototype website being developed. Users input the OTP code sent to the admin email received from the prototype website. Once users input their username and password, an OTP code will be sent to the administrator's email address. The next code is entered on the prototype web login page to access the prototype website administrator page and processed by the system to determine the information needed by the administrator. The research findings indicate that the prototype OTP-based website login system is implemented according to the developed algorithm, and the transmission of OTP codes is done through the administrator's email accessing the provided management portal, which will be done via email. Make sure the email address you enter matches the email address registered in the database system.

***Keyword:*** Network Security, Login Page, Email Notification