



UNIVERSITAS INDO GLOBAL MANDIRI PALEMBANG

**Implementasi *Two Factor Authentication* (2FA) Berdasarkan
Protokol RFC 3548 Menggunakan *Google Authenticator***

SKRIPSI

Halim Tri Anggoro

2017.11.0056

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER DAN SAINS
UNIVERSITAS INDO GLOBAL MANDIRI PALEMBANG**

2024



**Implementasi *Two Factor Authentication* (2FA) Berdasarkan
Protokol RFC 3548 Menggunakan *Google Authenticator***

SKRIPSI

**Diajukan Sebagai Syarat Untuk Menyelesaikan
Pendidikan Program Strata – 1 Pada
Program Studi Informatika**

Oleh:

Halim Tri Anggoro

2017.11.0056

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER DAN SAINS
UNIVERSITAS INDO GLOBAL MANDIRI PALEMBANG**

2024

LEMBAR PENGESAHAN SKRIPSI

LEMBAR PENGESAHAN SKRIPSI

Implementasi *Two Factor Authentication* (2FA) Berdasarkan
Protokol RFC 3548 Menggunakan *Google Authenticator*

Oleh

Halim Tri Anggoro
NPM : 2017.11.0056

Palembang , 02 September 20224

Pembimbing I



Rudi Heriansyah, S.T., M.Eng. Ph.D.
NIK : 2022.01.0315

Pembimbing II



Muhammad Haviz Irfani S.Si., M.T.I
NIK:2021.01.0291

Mengetahui,

Dekan Fakultas Ilmu Komputer dan Sains

FAKULTAS ILMU KOMPUTER DAN SAINS



Rudi Heriansyah, S.T., M.Eng. Ph.D.
NIK:2022.01.0315

LEMBAR PERSETUJUAN DEWAN PENGUJI

LEMBAR PERSETUJUAN DEWAN PENGUJI

Pada hari Rabu tanggal 21 Agustus 2024 telah dilaksanakan ujian sidang skripsi :

Nama : Halim Tri Anggoro
NPM : 2017.11.0056
Judul : Implementasi Two Factor Authentication (2FA) Berdasarkan Protokol RFC 3548 Menggunakan Google Authenticator

Oleh Prodi Teknik Informatika Fakultas Ilmu Komputer dan Sains Universitas Indo Global Mandiri Palembang

Palembang, 02 September 2024

Penguji 1,



Dr. Herri Setiawan, M.Kom
NIK: 2003.01.0060

Penguji 2,



Zaid Romegar Mair, S.T., M.Cs
NIK: 2021.01.0307

Penguji 3,



Muhasanah Rizvi Irani S.Si.,
M.T.
NIK: 2021.01.0291

Menyetujui,
Ka. Prodi Teknik Informatika



Zaid Romegar Mair, S.T., M.Cs
NIK: 2021.01.0307

SURAT KETERANGAN REVISI SKRIPSI



SURAT KETERANGAN REVISI SKRIPSI
PROGRAM STUDI TEKNIK INFORMATIKA (S1)
FASILKOM DAN SAINS UNIVERSITAS INDO GLOBAL MANDIRI

Kami yang bertanda tangan dibawah ini, menerangkan bahwa :

Nama : Halim Tri Anggoro
NPM : 2017.11.0056
Judul : Implementasi Two Factor Authentication (2FA) Berdasarkan
Protokol RFC 3548 Menggunakan Google Authenticator

Mahasiswa yang namanya tercantum diatas, telah selesai merevisi penulisan SKRIPSI

Palembang, 02 September 2024

Penguji 1,

Dr. Herri Setiawan, M.Kom
NIK: 2003.01.0060

Penguji 2,

Zaid Romegar Mair, S.T., M.Cs
NIK: 2021.01.0307

Penguji 3,

Muhammad Haviz Irfani S.Si., M.T.I.
NIK: 2021.01.0291

Menyetujui,
Ka. Prodi Teknik Informatika

Zaid Romegar Mair, S.T., M.Cs
NIK: 2021.01.0307

MOTTO DAN PERSEMBAHAN

MOTTO:

“Kemarin, saya merasa pintar. Oleh karena itu, saya ingin mengubah dunia. Tapi hari ini, saya menjadi orang yang lebih bijak. Oleh karena itu, saya mengubah diri saya sendiri” - Jalaluddin Rumi

PERSEMBAHAN:

Skripsi ini dipersembahkan kepada:

- ❖ Kepada almh ibu tercinta, dengan rasa hormat dan cinta yang mendalam, persembahan ini untukmu, ibu. Meski kini engkau telah pergi, kenangan dan kasih sayangmu tetap mengalir dalam hati dan jiwa ini. Engkau adalah sumber inspirasi dan kekuatan yang takkan pernah pudar.
- ❖ Kepada dosen pembimbing saya, Bapak Rudi Heriansyah, S.T., M.Eng. Ph.D. dan Bapak Muhammad Haviz Irfani S.Si., M.T.I yang memberi semangat serta sangat sabar dan selalu bersedia meluangkan waktu untuk membimbing saya agar bisa menyelesaikan skripsi ini.
- ❖ Kepada Ketua Prodi Teknik Informatika, Bapak Zaid Romegar Mair, S.T., M.Cs. Terimakasih telah memberikan saya kesempatan untuk bisa aktif kembali walaupun saya mengurus semester paling akhir ini melewati batas deadline. Dan juga saya selalu mengirimkan laporan melewati batas deadline. Terima kasih banyak pak, maaf selalu merepotkan.
- ❖ Kepada sahabat saya, Kristian Nugraha, M Rivaldo Dwi Putra dan Adli Heka Perdana. Terimakasih telah menjadi teman baik selama ini yang selalu mendengarkan keluh kesah saya.
- ❖ Kepada semua orang yang tidak bisa saya sebutkan satu persatu.

Implementasi *Two Factor Authentication* (2FA) Berdasarkan Protokol RFC 3548 Menggunakan *Google Authenticator*

ABSTRAK

Dengan banyaknya data yang tersimpan pada sistem aplikasi berbasis web yang rentan diakses oleh orang yang tidak berwenang, keamanan data menjadi sangat penting. *Two Factor Authentication* (2FA) menawarkan lapisan perlindungan tambahan dengan menggunakan dua metode otentikasi, yaitu sesuatu yang diketahui oleh pengguna (*password*) dan sesuatu yang dimiliki pengguna (kode otentikasi). Penelitian ini bertujuan untuk mengimplementasikan dan mengevaluasi keefektifan dari sistem *Two Factor Authentication* (2FA) berbasis *Google Authenticator* yang diimplementasikan menggunakan skenario dari serangan *Brute Force* dan *SQL Injection*. Metode pengembangan yang digunakan dalam penelitian ini adalah *Software Development Life Cycle* (SDLC) model *Waterfall*, yang mencakup tahapan analisis kebutuhan, desain sistem, implementasi, dan pengujian. Sistem yang dibangun memanfaatkan algoritma *Time-Based One-Time Password* (TOTP) untuk menghasilkan kode otentikasi yang *valid* dalam *interval* waktu tertentu. Hasil penelitian menunjukkan bahwa implementasi 2FA ini berhasil meningkatkan keamanan akses sistem secara signifikan, namun tetap ada potensi kelemahan yang perlu diperhatikan, terutama terkait dengan keamanan penyimpanan *secret key*. Penelitian ini memberikan kontribusi dalam memberikan solusi keamanan untuk aplikasi web.

Kata Kunci: *Two Factor Authentication*, *Google Authenticator*, *Time-Based One-Time Password*, Keamanan Aplikasi Web.

Implementation of Two Factor Authentication (2FA) Based on RFC 3548 Protocol Using Google Authenticator

ABSTRACT

With a lot of data stored on web-based application systems that are vulnerable to access by unauthorized people, data security is very important. Two Factor Authentication (2FA) offers an additional layer of protection by using two authentication methods, namely something known by the user (password) and something owned by the user (authentication code). This research aims to implement and evaluate the effectiveness of the Google Authenticator-based Two Factor Authentication (2FA) system implemented using scenarios from Brute Force and SQL Injection attacks. The development method used in this research is the Software Development Life Cycle (SDLC) Waterfall model, which includes the stages of requirements analysis, system design, implementation, and testing. The system built utilizes the Time-Based One-Time Password (TOTP) algorithm to generate valid authentication codes within a certain time interval. The results show that the implementation of 2FA has significantly improved the security of system access, but there are still potential weaknesses that need to be considered, especially related to the security of secret key storage. This research contributes to providing security solutions for web applications.

Keywords: *Two Factor Authentication, Google Authenticator, Time-Based One-Time Password, Web Application Security.*

KATA PENGANTAR

Puji dan Syukur Penulis persembahkan kepada Allah SWT karena berkat Rahmat dan Hidayah-Nyalah akhirnya penelitian ini bisa terselesaikan dengan baik tepat pada waktunya, tidak lupa shalawat serta salam selalu dilimpahkan kepada junjungan kita Nabi Muhammad SAW beserta keluarga sahabat para pengikut dan insyaallah kita semua hingga akhir zaman.

Skripsi yang Penulis buat dengan judul “**Implementasi *Two Factor Authentication* (2FA) Berdasarkan Protokol RFC 3548 Menggunakan *Google Authenticator***” disusun guna memenuhi syarat kelulusan dalam memperoleh gelar Sarjana (S1) pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer dan Sains, Universitas Indo Global Mandiri (UIGM) Palembang.

Tidak lupa Penulis mengucapkan terima kasih atas bantuan yang diberikan selama penyusunan skripsi ini kepada:

1. Bapak Dr. Marzuki Alie, SE., MM, selaku Rektor Universitas Indo Global Mandiri Palembang.
2. Bapak Rudi Heriansyah, S.T., M.Eng. Ph.D. sebagai Dekan Fakultas Ilmu komputer dan Sains dan sebagai Dosen Pembimbing I.
3. Bapak Zaid Romegar Mair, S.T., M.Cs. sebagai Ketua Prodi Teknik Informatika Universitas Indo Global Mandiri Palembang.
4. Bapak Muhammad Haviz Irfani S.Si., M.T.I sebagai Dosen Pembimbing II.
5. Ibu Septa Cahyani, S.Kom., M.Cs. sebagai Pembimbing Akademik.
6. Bapak/Ibu Dosen Fakultas Ilmu Komputer dan Sains dan karyawan/karyawati Universitas Indo Global Mandiri Palembang.

Penulis menyadari bahwa penyusunan skripsi ini masih memiliki banyak kekurangan, karenanya Penulis mengharapkan saran dan kritik yang sifatnya membangun agar dapat digunakan demi perbaikan skripsi ini nantinya. Penulis juga

berharap agar skripsi ini akan memberikan banyak manfaat bagi semua pihak yang memerlukannya.

Palembang, 29 Maret 2024

Penulis,

Halim Tri Anggoro

DAFTAR ISI

HALAMAN JUDUL LUAR	i
HALAMAN JUDUL DALAM	ii
LEMBAR PENGESAHAN SKRIPSI	iii
LEMBAR PERSETUJUAN DEWAN PENGUJI	iv
SURAT KETERANGAN REVISI SKRIPSI	v
MOTTO DAN PERSEMBAHAN	vi
ABSTRAK	vii
ABSTRACT	viii
KATA PENGANTAR	ix
DAFTAR ISI	xi
DAFTAR GAMBAR	xiv
DAFTAR TABEL	xvii
DAFTAR LAMPIRAN	xviii
BAB 1 PENDAHULUAN	
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah.....	2
1.4 Tujuan dan Manfaat.....	2
1.4.1 Tujuan Penelitian	2
1.4.2 Manfaat Penelitian	3
1.5 Sistematika Penulisan.....	3
BAB 2 LANDASAN TEORI	
2.1 <i>Two-Factor Authentication</i>	5
2.2 Jenis – Jenis <i>One Time Password</i>	6
2.2.1 <i>One-Time Password (OTP)</i>	6
2.2.2 <i>HMAC-Based One-Time Password (HOTP)</i>	7

2.2.3 <i>Time-Based One-Time Password (TOTP)</i>	7
2.3 <i>Algoritma Time-Based One-Time Password (TOTP)</i>	7
2.4 RFC 3548	9
2.4.1 <i>Base16</i>	9
2.4.2 <i>Base32</i>	10
2.4.3 <i>Base64</i>	10
2.5 <i>Pembangkit Bilangan Acak</i>	10
2.6 <i>QR Code</i>	11
2.7 <i>Aplikasi Google Authenticator</i>	11
2.8 <i>SQL Injection</i>	12
2.9 <i>Brute Force</i>	12
2.10 <i>Web</i>	13
2.10.1 <i>Pemrograman Web</i>	13
2.10.2 <i>XAMPP dan PHP</i>	14
2.10.3 <i>Basis Data, SQL dan MySQL</i>	14
2.11 <i>Model Pengembangan Perangkat Lunak</i>	15
2.12 <i>Unified Modeling Language (UML)</i>	17
2.12.1 <i>Use Case Diagram</i>	17
2.12.2 <i>Activity Diagram</i>	19
2.12.3 <i>Class Diagram</i>	20
2.12.4 <i>Sequence Diagram</i>	22
2.13 <i>Pengujian Perangkat Lunak</i>	24
2.13.1 <i>Black Box Testing</i>	24
2.14 <i>Flowchart</i>	25
2.15 <i>Penelitian Terdahulu</i>	27

BAB 3 METODOLOGI PENELITIAN

3.1 <i>Tahapan Penelitian</i>	30
3.2 <i>Pengumpulan Data</i>	32

3.3 Model Pengembangan Sistem	33
3.3.1 Analisis Kebutuhan Sistem.....	33
3.3.2 Desain Sistem	35
3.3.3 Desain Tampilan Antarmuka.....	40
BAB 4 HASIL DAN PEMBAHASAN	
4.1 Pengkodean	43
4.2 Pengujian.....	46
4.3 Analisis Sistem.....	49
4.3.1 Algoritma <i>Time-Based One-Time Password</i> (TOTP)	50
4.3.2 Analisis Cara Kerja Sistem.....	56
4.3.3 <i>Aktivasi Dan Verifikasi</i> Pengguna	77
4.3.4 Analisis Kekuatan Sistem.....	81
4.3.5 Analisis Kelemahan Sistem	83
BAB 5 PENUTUP	
5.1 Kesimpulan.....	88
5.2 Saran.....	88
DAFTAR PUSTAKA	90
LAMPIRAN	

DAFTAR GAMBAR

Gambar 2.1 Contoh <i>QR Code</i>	11
Gambar 2.2 Logo Aplikasi <i>Google Authenticator</i>	12
Gambar 2.3 Ilustrasi Model <i>Waterfall</i>	16
Gambar 3.1 Tahapan Penelitian.....	30
Gambar 3.2 <i>Flowchart</i> Sistem Umum.....	35
Gambar 3.3 <i>Use Case Diagram</i>	36
Gambar 3.4 <i>Activity Diagram</i>	37
Gambar 3.5 <i>Class Diagram</i>	38
Gambar 3.6 <i>Sequence Diagram</i>	39
Gambar 3.7 Desain Tampilan <i>Registrasi</i>	40
Gambar 3.8 Desain Tampilan <i>Login</i>	41
Gambar 3.9 Desain Tampilan <i>Aktivasi 2FA</i>	41
Gambar 3.10 Desain Tampilan <i>Verifikasi 2FA</i>	42
Gambar 3.11 Desain Tampilan <i>Dashboard</i>	42
Gambar 4.1 Halaman <i>Registrasi</i>	43
Gambar 4.2 Halaman <i>Login</i>	44
Gambar 4.3 Halaman <i>Aktivasi</i>	45
Gambar 4.4 Halaman <i>Verifikasi</i>	45
Gambar 4.5 Halaman <i>Dashboard</i>	46
Gambar 4.6 Waktu Dan Langkah Waktu.....	51
Gambar 4.7 Waktu Unix.....	51
Gambar 4.8 Berbagi Kunci.....	56
Gambar 4.9 <i>Flowchart</i> Halaman <i>Registrasi</i>	57
Gambar 4.10 <i>Flowchart creatSecret</i>	58
Gambar 4.11 <i>Flowchart _getBase32LookupTable</i>	58
Gambar 4.12 Tampilan Halaman <i>Registrasi</i>	59

Gambar 4.13 Potongan Kode Program Halaman <i>Registrasi</i>	59
Gambar 4.14 Potongan Kode Program Halaman <i>Registrasi (Lanjutan)</i>	60
Gambar 4.15 Kode Program <i>creatSecret</i>	61
Gambar 4.16 Kode Program <i>_getBase32LookupTable</i>	62
Gambar 4.17 <i>Flowchart</i> Halaman <i>Aktivasi/Verifikasi</i>	63
Gambar 4.18 <i>Flowchart</i> <i>getQRCodeGoogleUrl</i>	64
Gambar 4.19 Tampilan Halaman <i>Aktivasi/Verifikasi</i>	65
Gambar 4.20 Potongan Kode Program Halaman <i>Aktivasi/Verifikasi</i>	65
Gambar 4.21 Potongan Kode Program Halaman <i>Aktivasi/Verifikasi (Lanjutan)</i>	66
Gambar 4.22 Kode Program <i>getQRCodeGoogleUrl</i>	66
Gambar 4.23 <i>Flowchart</i> <i>Auth.php</i>	68
Gambar 4.24 <i>Flowchart</i> <i>verifCode</i>	69
Gambar 4.25 <i>Flowchart</i> <i>getCode</i>	70
Gambar 4.26 <i>Flowchart</i> <i>_base32Decode</i>	71
Gambar 4.27 <i>Flowchart</i> <i>_getBase32LookupTable</i>	72
Gambar 4.28 <i>Flowchart</i> <i>setCodeLength</i>	72
Gambar 4.29 Kode Program <i>Auth.php</i>	73
Gambar 4.30 Kode Program <i>verifCode</i>	74
Gambar 4.31 Kode Program <i>getCode</i>	75
Gambar 4.32 Kode Program <i>_base32Decode</i>	76
Gambar 4.33 Kode Program <i>setCodeLength</i>	77
Gambar 4.34 Memindai <i>QR Code</i>	78
Gambar 4.35 Mengetikkan Kode TOTP.....	79
Gambar 4.36 Masukkan Kode TOTP	80
Gambar 4.37 Akses Melalui Tebakan <i>Username</i> dan <i>Password</i>	81
Gambar 4.38 Akses Ditolak Karena Autentikasi Dua Faktor	82
Gambar 4.39 Penguasaan Database Melalui <i>SQL Injection</i>	84
Gambar 4.40 Autentikasi Dua Faktor Menghambat Akses	84
Gambar 4.41 <i>Eksplorasi</i> Kelemahan dalam Autentikasi Dua Faktor	85

Gambar 4.42 Menghasilkan Kode Autentikasi dengan TOTP Token *Generator* 86

Gambar 4.43 Akses Berhasil ke Sistem Melalui *Eksplorasi Secret Key* 87

DAFTAR TABEL

Tabel 2.1 Simbol <i>Use Case Diagram</i>	18
Tabel 2.2 Simbol <i>Activity Diagram</i>	19
Tabel 2.3 Simbol <i>Class Diagram</i>	20
Tabel 2.4 Simbol <i>Sequence Diagram</i>	22
Tabel 2.5 Simbol Diagram <i>Flowchart</i>	25
Tabel 2.6 Penelitian Terdahulu.....	27
Tabel 3.1 Tabel <i>User</i>	39
Tabel 4.1 Pengujian Halaman <i>Registrasi</i>	47
Tabel 4.2 Pengujian Halaman <i>Login</i>	47
Tabel 4.3 Pengujian Halaman <i>Aktivasi</i>	48
Tabel 4.4 Pengujian Halaman <i>Verifikasi</i>	49
Tabel 4.5 Contoh Hasil Perhitungan TOTP	53
Tabel 4.6 Kemungkinan Kombinasi Angka	83

DAFTAR LAMPIRAN

LAMPIRAN 1 LEMBAR PENGESAHAN SKRIPSI

LAMPIRAN 2 LEMBAR PERSETUJUAN DEWAN PENGUJI

LAMPIRAN 3 SURAT KETERANGAN REVISI SKRIPSI

LAMPIRAN 4 SURAT KETERANGAN SIAP SIDANG SKRIPSI

LAMPIRAN 5 SURAT PERSETUJUAN SIDANG SKRIPSI

LAMPIRAN 6 BIOGRAFI PENULIS

LAMPIRAN 7 KARTU BIMBINGAN

LAMPIRAN 8 PERNYATAAN TIDAK PLAGIAT

LAMPIRAN 9 KODE PROGRAM