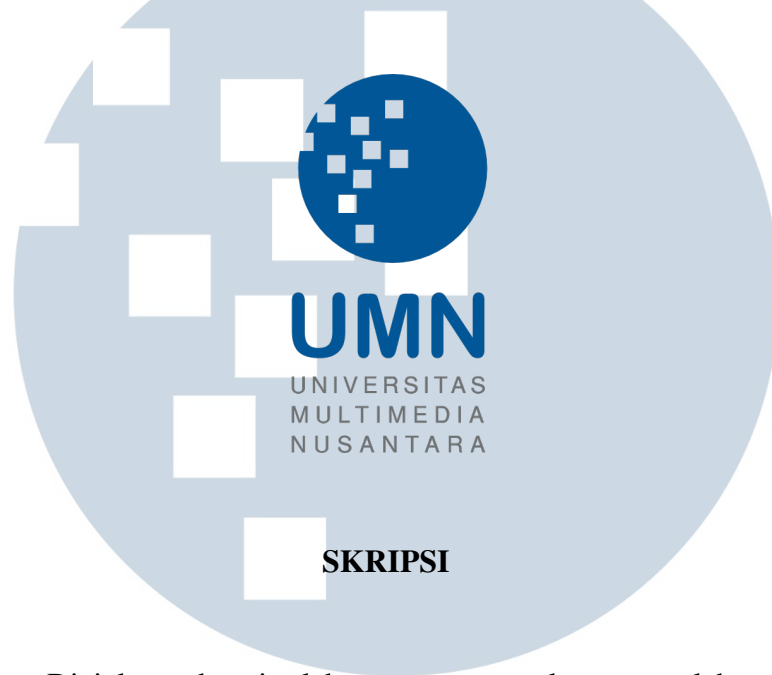


**IMPLEMENTASI TIME-BASED ONE-TIME PASSWORD
MENGUNAKAN CHALLENGE RESPONSE AUTHENTICATION
MECHANISM UNTUK KEAMANAN TRANSAKSI DIGITAL APLIKASI
ANDROID**



SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh
Gelar Sarjana Komputer (S.Kom.)

Andrian Santo
0000027833

UMN

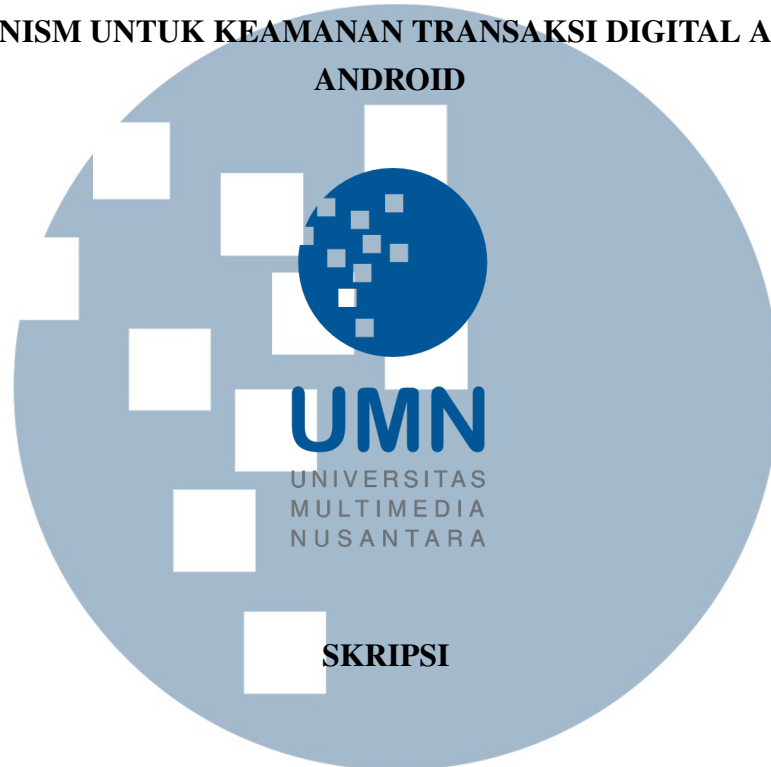
**UNIVERSITAS
MULTIMEDIA
NUSANTARA**

**PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS MULTIMEDIA NUSANTARA**

TANGERANG

2022

**IMPLEMENTASI TIME-BASED ONE-TIME PASSWORD
MENGUNAKAN CHALLENGE RESPONSE AUTHENTICATION
MECHANISM UNTUK KEAMANAN TRANSAKSI DIGITAL APLIKASI
ANDROID**



Diajukan sebagai salah satu syarat untuk memperoleh
Gelar Sarjana Komputer (S.Kom.)

Andrian Santo
0000027833

UMN

UNIVERSITAS

MULTIMEDIA

NUSANTARA

**PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS MULTIMEDIA NUSANTARA**

TANGERANG

2022

HALAMAN PERNYATAAN TIDAK PLAGIAT

Dengan ini saya,

Nama : Andrian Santo
Nomor Induk Mahasiswa : 00000027833
Program Studi : Informatika

Skripsi dengan judul:

Implementasi Time-based One-Time Password Menggunakan Challenge Response Authentication Mechanism untuk Keamanan Transaksi Digital Aplikasi Android

merupakan hasil karya saya sendiri bukan plagiat dari karya ilmiah yang ditulis oleh orang lain, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar serta dicantumkan di Daftar Pustaka.

Jika di kemudian hari terbukti ditemukan kecurangan/ penyimpangan, baik dalam pelaksanaan Skripsi maupun dalam penulisan laporan Skripsi, saya bersedia menerima konsekuensi dinyatakan TIDAK LULUS untuk Tugas akhir yang telah saya tempuh.

Tangerang, 10 Juni 2022



(Andrian Santo)

UMM
UNIVERSITAS
MULTIMEDIA
NUSANTARA

HALAMAN PENGESAHAN

Skripsi dengan judul

**IMPLEMENTASI TIME-BASED ONE-TIME PASSWORD
MENGUNAKAN CHALLENGE RESPONSE AUTHENTICATION
MECHANISM UNTUK KEAMANAN TRANSAKSI DIGITAL APLIKASI
ANDROID**

oleh

Nama : Andrian Santo
NIM : 00000027833
Program Studi : Informatika
Fakultas : Fakultas Teknik dan Informatika

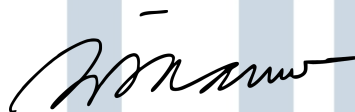
Telah diujikan pada hari Selasa, 21 Juni 2022

Pukul 13.00 s/d 15.00 dan dinyatakan

LULUS

Dengan susunan penguji sebagai berikut

Ketua Sidang



(Dr. Winarno, M.Kom.)

NIDN: 330106002

Penguji



(Dr. Ni Made Satvika Iswari, S.T., M.T.)

NIDN: 0306019001

Pembimbing

UNIVERSITAS
MULTIMEDIA
NUSANTARA

(Yaman Khaeruzzaman, M.Sc.)

NIDN: 0413057104

Ketua Program Studi Informatika,

(Marlinda Vasty Overbeek, S.Kom., M.Kom.)

NIDN: 0818038501

**HALAMAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK
KEPENTINGAN AKADEMIS**

Sebagai sivitas akademik Universitas Multimedia Nusantara, saya yang bertanda tangan di bawah ini:

Nama : Andrian Santo
NIM : 00000027833
Program Studi : Informatika
Fakultas : Teknik dan Informatika
Jenis Karya : Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada **Universitas Multimedia Nusantara** hak Bebas Royalti Non-eksklusif (*Non-exclusive Royalty-Free Right*) atas karya ilmiah saya yang berjudul:

**IMPLEMENTASI TIME-BASED ONE-TIME PASSWORD
MENGUNAKAN CHALLENGE RESPONSE AUTHENTICATION
MECHANISM UNTUK KEAMANAN TRANSAKSI DIGITAL APLIKASI
ANDROID**

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non eksklusif ini Universitas Multimedia Nusantara berhak menyimpan, mengalih media / format-kan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis / pencipta dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

Tangerang, 10 Juni 2022

Yang menyatakan

UNIVERSITAS
MULTIMEDIA
NUSANTARA



Andrian Santo

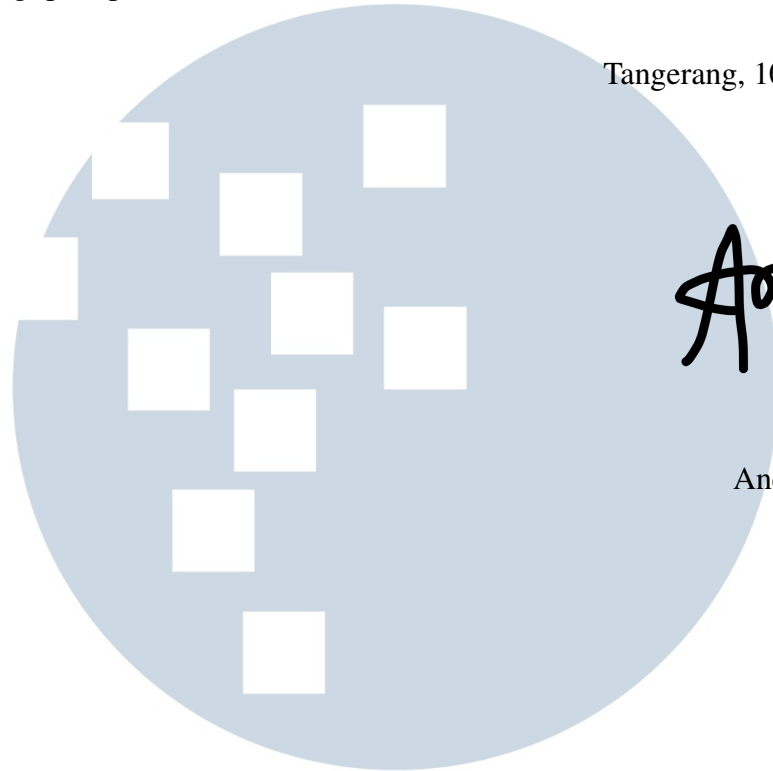
KATA PENGANTAR

Puji Syukur atas berkat dan rahmat kepada Tuhan Yang Maha Esa, atas selesainya penulisan laporan Skripsi ini dengan judul: Implementasi Time-based One-Time Password Menggunakan Challenge Response Authentication Mechanism untuk Keamanan Transaksi Digital Aplikasi Android dilakukan untuk memenuhi salah satu syarat untuk mencapai gelar Sarjana Komputer Jurusan Informatika Pada Fakultas Teknik dan Informatika Universitas Multimedia Nusantara. Saya menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan skripsi ini, sangatlah sulit bagi saya untuk menyelesaikan skripsi ini. Oleh karena itu, saya mengucapkan terima kasih kepada:

1. Bapak Dr. Ninok Leksono, selaku Rektor Universitas Multimedia Nusantara.
2. Dr. Eng. Niki Prastomo, S.T., M.Sc., selaku Dekan Fakultas Teknik dan Informatika Universitas Multimedia Nusantara.
3. Ibu Marlinda Vasty Overbeek, S.Kom., M.Kom., selaku Ketua Program Studi Informatika Universitas Multimedia Nusantara.
4. Bapak Yaman Khaeruzzaman, M.Sc., sebagai Pembimbing pertama yang telah banyak meluangkan waktu untuk memberikan bimbingan, arahan dan motivasi atas terselesainya tesis ini.
5. Kepada Papa, Mama, dan Adik, yang telah memberikan bantuan dukungan material serta motivasi, sehingga saya menyelesaikan laporan magang ini.
6. Kepada teman-teman dari Sel Isidorus KTM MM Serpong, yang telah memberikan doa dan dukungan motivasi.
7. Kepada James Leopold dan Zefanya Wijaya, yang telah menemani, membantu, dan memberikan dukungan motivasi dari awal kuliah hingga tesis ini bisa berhasil dibuat.
8. Kepada Brenda Estherina dan Kezia, yang memberikan dukungan motivasi, awal penyusunan tesis hingga tesis ini bisa berhasil dibuat.
9. Kepada para responden, yang telah membantu serta meluangkan waktu untuk mengisi kuisioner yang digunakan untuk tesis ini.

Semoga skripsi ini bermanfaat, baik sebagai sumber informasi maupun sumber inspirasi, bagi para pembaca.

Tangerang, 10 Juni 2022



Andrian Santo

Andrian Santo

UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA

**IMPLEMENTASI TIME-BASED ONE-TIME PASSWORD
MENGUNAKAN CHALLENGE RESPONSE AUTHENTICATION
MECHANISM UNTUK KEAMANAN TRANSAKSI DIGITAL APLIKASI**

ANDROID

Andrian Santo

ABSTRAK

Internet telah memberi banyak kemudahan kepada masyarakat dalam melakukan berbagai kegiatan. Melalui internet, pengguna dapat melakukan berbagai transaksi digital seperti berbelanja, *top-up*, pengiriman dana, dan masih banyak lainnya. Namun dibalik banyaknya kemudahan dan kecanggihan fasilitas yang digunakan, terdapat beberapa masalah yang terjadi. Terutama dalam hal keamanan. Banyak perusahaan telah melakukan optimasi sistem keamanan transaksinya agar masyarakat menjadi lebih aman dan nyaman dalam melakukan transaksi. Tetapi, bagi sebagian masyarakat optimasi tersebut masih belum optimal dikarenakan terdapat banyaknya kasus pencurian data pengguna dan dana yang hilang. Terutama salah satu penyebabnya adalah kehilangan telepon pintar. Oleh karena itu, penelitian ini dilakukan untuk mengimplementasikan sebuah sistem keamanan tambahan untuk melindungi pengguna dari permasalahan tersebut melalui penggunaan *Time-Based One-Time Password (TOTP)* dengan *Challenge Response Authentication Mechanism (CRAM)* yang diuji dalam simulasi pada aplikasi Android. Simulasi aplikasi ini telah berhasil dirancang dan dibangun, serta dalam pengujian aplikasi ini mendapatkan hasil sebesar 89,68% menggunakan penerapan metode keamanan TOTP dengan CRAM.

Kata kunci: *Android, Challenge Response Authenticaiton Mechanism, Time-Based One-Time Password, Transaksi Digital.*

U N I V E R S I T A S
M U L T I M E D I A
N U S A N T A R A

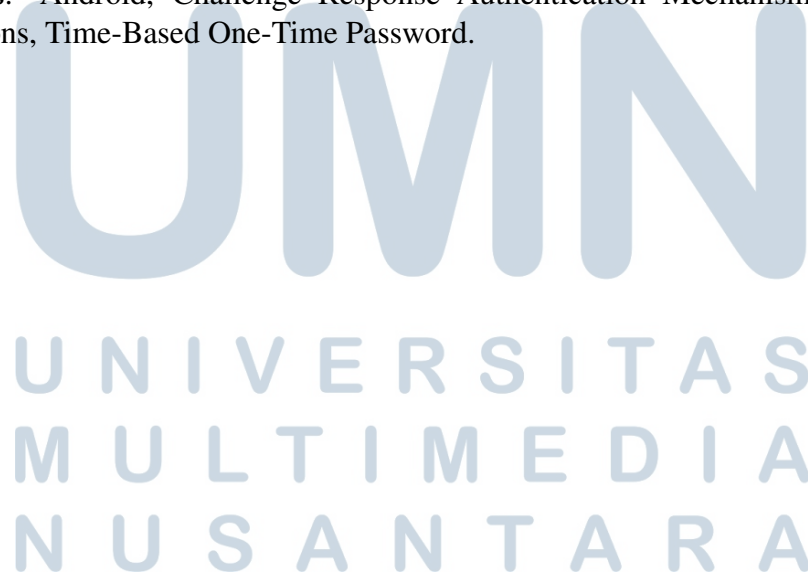
IMPLEMENTATION OF TIME-BASED ONE-TIME PASSWORD USING CHALLENGE RESPONSE AUTHENTICATION MECHANISM FOR ANDROID APPLICATION DIGITAL TRANSACTION SECURITY

Andrian Santo

ABSTRACT

The internet has made it easier for people to carry out various activities. Through the internet, users can perform various digital transactions such as shopping, top-up, sending funds, and many others. But behind the many conveniences and sophistication of the facilities used, there are several problems that occur. Especially in terms of security. Many companies have optimized their transaction security systems so that people become more secure and comfortable in conducting transactions. However, for some people the optimization is still not optimal because there are many cases of user data has been stolen and lost funds. Mainly one of the causes is the loss of a smartphone. Therefore, this research was conducted to implement an additional security system to protect users from these problems through the use of Time-Based One-Time Password (TOTP) with Challenge Response Authentication Mechanism (CRAM) which was tested in simulation on Android applications. This application simulation has been successfully designed and built, also during testing this application, the results obtained are 89.68% using the application of the TOTP security method with CRAM.

Keywords: Android, Challenge Response Authentication Mechanism, Digital Transactions, Time-Based One-Time Password.



DAFTAR ISI

HALAMAN JUDUL	i
PERNYATAAN TIDAK MELAKUKAN PLAGIAT	ii
HALAMAN PENGESAHAN	iii
HALAMAN PERSETUJUAN PUBLIKASI ILMIAH	iv
KATA PENGANTAR	v
ABSTRAK	vii
ABSTRACT	viii
DAFTAR ISI	ix
DAFTAR GAMBAR	xi
DAFTAR TABEL	xiii
DAFTAR LAMPIRAN	xiv
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	3
1.3 Batasan Permasalahan	3
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	3
1.6 Sistematika Penulisan	4
BAB 2 LANDASAN TEORI	6
2.1 Metode Waterfall	6
2.2 Android	8
2.3 Retrofit	8
2.4 Firebase	8
2.4.1 Firebase Authentication	8
2.4.2 Firebase Firestore Database	9
2.5 Node JS	9
2.5.1 React JS	9
2.5.2 Express JS	10
2.5.3 Express Rate Limiter	10
2.5.4 Crypto	10
2.6 Metode One-Time Password (OTP)	10
2.6.1 One-Time Password	10
2.6.2 Hmac-based One-Time Password (HOTP)	11
2.6.3 Time-based One-Time Password (TOTP)	11
2.7 Challenge Response Authentication Mechanism (CRAM)	13
2.8 Github	14
2.9 Vercel	14
2.10 Black Box Testing	15
2.11 End User Computing Satisfaction	15
2.12 Skala Likert	17
BAB 3 METODOLOGI PENELITIAN	19
3.1 Analisis Kebutuhan Sistem	19
3.1.1 Kebutuhan Fungsional	19
3.1.2 Kebutuhan Non Fungsional	20
3.2 Perancangan Aplikasi	20
3.2.1 Diagram Alir	21
3.2.2 Struktur Database	36
3.2.3 Mockup Aplikasi	38

BAB 4	HASIL DAN DISKUSI	51
4.1	Implementasi Sistem	51
4.1.1	Implementasi Database	51
4.1.2	Implementasi Aplikasi	53
4.1.3	Implementasi Website	70
4.1.4	Source Code	74
4.2	Realisasi Fungsional Aplikasi	91
4.3	Black Box Testing	91
4.3.1	Pengujian Aplikasi	92
4.3.2	Pengujian Web	101
4.4	Evaluasi Aplikasi	105
BAB 5	SIMPULAN DAN SARAN	108
5.1	Simpulan	108
5.2	Saran	108
DAFTAR PUSTAKA	110



DAFTAR GAMBAR

Gambar 2.1	Tahapan Metode Waterfall	6
Gambar 2.2	Diagram Alir CRAM	13
Gambar 2.3	Model Evaluasi <i>End User Computing Satisfaction</i>	16
Gambar 3.1	Diagram Alir Alur <i>Dynamic</i>	21
Gambar 3.2	Diagram Alir Alur <i>Static</i>	22
Gambar 3.3	Diagram Alir Halaman <i>Login</i> Aplikasi	23
Gambar 3.4	Diagram Alir Halaman <i>Register</i> Aplikasi	25
Gambar 3.5	Diagram Alir Halaman <i>Secret ID</i> Aplikasi	27
Gambar 3.6	Diagram Alir Halaman <i>Home</i> Aplikasi	28
Gambar 3.7	Diagram Alir Halaman <i>Search</i> Aplikasi	29
Gambar 3.8	Diagram Alir Halaman <i>Detail</i> Produk Aplikasi	30
Gambar 3.9	Diagram Alir Halaman Konfirmasi Aplikasi	31
Gambar 3.10	Diagram Alir Halaman <i>TOTP</i> Aplikasi	32
Gambar 3.11	Diagram Alir Halaman <i>Generate OTP Code</i>	33
Gambar 3.12	Diagram Alir Halaman <i>Login Web</i>	34
Gambar 3.13	Diagram Alir Halaman <i>TOTP Web</i>	35
Gambar 3.14	Diagram Alir Halaman <i>Receipt</i> Aplikasi	36
Gambar 3.15	Firestore Authentication	37
Gambar 3.16	<i>Mockup</i> Halaman <i>Login</i>	39
Gambar 3.17	<i>Mockup</i> Halaman <i>Register</i>	40
Gambar 3.18	<i>Mockup</i> Halaman <i>Secret ID</i>	41
Gambar 3.19	<i>Mockup</i> Halaman Konfirmasi <i>Secret ID</i>	42
Gambar 3.20	<i>Mockup</i> Halaman <i>Home</i>	43
Gambar 3.21	<i>Mockup</i> Halaman <i>Search</i>	44
Gambar 3.22	<i>Mockup</i> Halaman <i>Detail Product</i>	45
Gambar 3.23	<i>Mockup</i> Halaman Konfirmasi	46
Gambar 3.24	<i>Mockup</i> Halaman <i>OTP</i>	47
Gambar 3.25	<i>Mockup</i> Halaman <i>Receipt</i>	48
Gambar 3.26	<i>Mockup</i> Halaman <i>Login</i>	49
Gambar 3.27	<i>Mockup</i> Halaman <i>TOTP</i>	50
Gambar 4.1	Implementasi Firestore Authentication	51
Gambar 4.2	Implementasi Firestore Database Tabel User Data	52
Gambar 4.3	Implementasi Firestore Database Tabel User Second	52
Gambar 4.4	Implementasi Halaman Login	53
Gambar 4.5	Implementasi Halaman Login (Toast Enter Email and Password)	54
Gambar 4.6	Implementasi Halaman Login (Toast Login Failed)	54
Gambar 4.7	Implementasi Halaman Register	55
Gambar 4.8	Implementasi Halaman Register (Toast Enter Value)	56
Gambar 4.9	Implementasi Halaman Register (Toast Enter Valid Email)	57
Gambar 4.10	Implementasi Halaman Register (Toast password do not match)	57
Gambar 4.11	Implementasi Halaman Register (Toast Register Failed)	58
Gambar 4.12	Implementasi Halaman Secret ID	59
Gambar 4.13	Implementasi Halaman Secret ID Confirm	59
Gambar 4.14	Implementasi Halaman Home	60
Gambar 4.15	Implementasi Halaman Search	61

Gambar 4.16	Implementasi Halaman Detail Produk	62
Gambar 4.17	Implementasi Halaman Konfirmasi	63
Gambar 4.18	Implementasi Halaman TOTP (awal)	64
Gambar 4.19	Implementasi Halaman TOTP	64
Gambar 4.20	Implementasi Halaman TOTP (Send Again)	65
Gambar 4.21	Implementasi Halaman TOTP (Code Limited)	66
Gambar 4.22	Implementasi Halaman TOTP (Input)	67
Gambar 4.23	Implementasi Halaman TOTP (Success)	68
Gambar 4.24	Implementasi Halaman Receipt	69
Gambar 4.25	Implementasi Halaman Login Web	70
Gambar 4.26	Implementasi Halaman Login Web (Please Fill)	71
Gambar 4.27	Implementasi Halaman Login Web (Please Check)	71
Gambar 4.28	Implementasi Halaman OTP Web	72
Gambar 4.29	Implementasi Web Backend	73
Gambar 4.30	Implementasi Web Backend (Limit)	73
Gambar 4.31	Source Code View Pager	74
Gambar 4.32	Source Code Check Login	74
Gambar 4.33	Source Code Check Register Data	75
Gambar 4.34	Source Code Generate Secret ID	76
Gambar 4.35	Source Code Register	77
Gambar 4.36	Source Code MainActivity Get User Data	78
Gambar 4.37	Source Code Halaman Konfirmasi Popup	79
Gambar 4.38	Source Code Search Filter	80
Gambar 4.39	Source Code Get Current Time	80
Gambar 4.40	Source Code Start Timer	81
Gambar 4.41	Source Code Send Again	81
Gambar 4.42	Source Code Check Code	82
Gambar 4.43	Source Code Get API Interface	82
Gambar 4.44	Source Code Fetch Data	83
Gambar 4.45	Source Code Save OTP	84
Gambar 4.46	Source Code Check Entered OTP	84
Gambar 4.47	Source Code Verify OTP (Call)	85
Gambar 4.48	Source Code Verify OTP (Check)	85
Gambar 4.49	Source Code Verify OTP (Change Balance)	85
Gambar 4.50	Source Code Verify OTP	86
Gambar 4.51	Source Code Web Frontend Router	86
Gambar 4.52	Source Code Web Frontend Firebase	87
Gambar 4.53	Source Code Web Frontend Login	87
Gambar 4.54	Source Code Web Frontend Logout	88
Gambar 4.55	Source Code Web Frontend OTP	88
Gambar 4.56	Source Code Web Frontend Fetch Data	89
Gambar 4.57	Source Code Web Frontend Fetch Data (Date)	89
Gambar 4.58	Source Code Web Backend Rate Limiter	90
Gambar 4.59	Source Code Web Backend Endpoint	90
Gambar 4.60	Source Code Web Backend Get Random Number	91

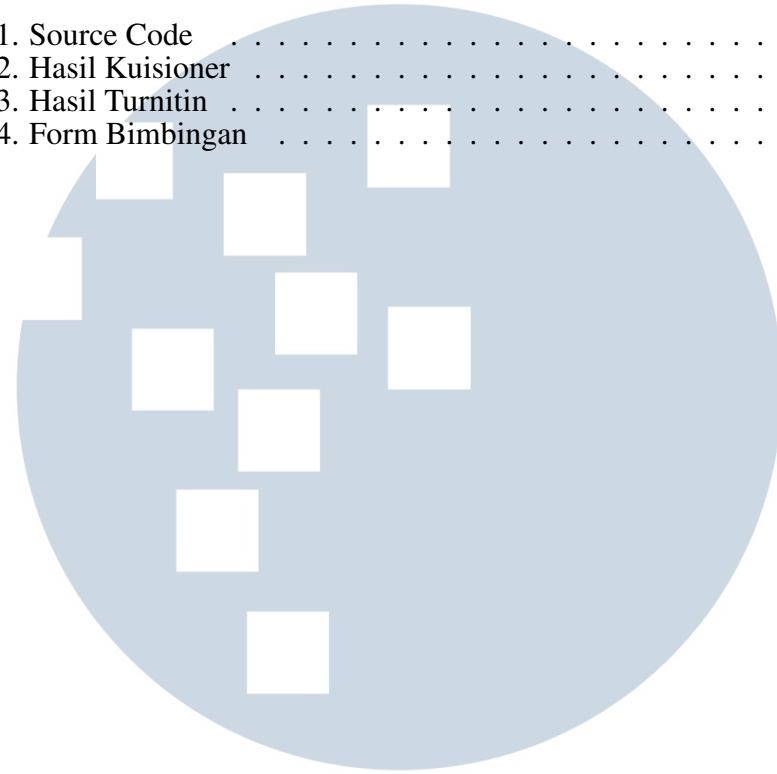
DAFTAR TABEL

Tabel 2.1	Kriteria Skala Likert	17
Tabel 3.1	Firebase Firestore Database User Data	38
Tabel 3.2	Firebase Firestore Database User Second	38
Tabel 4.1	Realisasi Kebutuhan Sistem	91
Tabel 4.2	Pengujian Aplikasi	92
Tabel 4.3	Pengujian Web Frontend	101
Tabel 4.4	Pengujian Web Backend	104
Tabel 4.5	Daftar Pertanyaan Kuisisioner	105
Tabel 4.6	Jawaban Pertanyaan Kuesioner	106



DAFTAR LAMPIRAN

Lampiran 1. Source Code	112
Lampiran 2. Hasil Kuisisioner	113
Lampiran 3. Hasil Turnitin	119
Lampiran 4. Form Bimbingan	120



UMN

UNIVERSITAS
MULTIMEDIA
NUSANTARA