

ABSTRAK

Abiel Nathanael Georgius Pasaribu:

Tugas Akhir

Prototipe Penerapan Zero Trust Berbasis Autentikasi Multi-Faktor untuk Meningkatkan Keamanan pada Aplikasi *My Petra*

Perlindungan terhadap sistem informasi akademik sangat penting untuk mencegah kebocoran data akibat serangan siber, termasuk upaya login berulang (*brute-force*), akses tanpa izin, maupun penggunaan kata sandi bawaan yang belum diganti. Universitas Kristen Petra telah menggantikan metode autentikasi *Single Sign-On (SSO)* dengan *Lightweight Directory Access Protocol (LDAP)* untuk meningkatkan keamanan akses aplikasi *My Petra*. Penelitian ini mengembangkan prototipe sistem autentikasi berbasis *Zero Trust Architecture (ZTA)* dengan *Multi-Factor Authentication (MFA)* menggunakan *Laravel* sebagai *backend* dan *Blade* sebagai antarmuka pengguna, serta dihosting pada *cPanel* untuk pengujian. Sistem ini menggunakan autentikasi *OTP (One-Time Password)* melalui *Google Authenticator*, *email*, dan *SMS/Whatsapp*, dilengkapi dengan *Trusted Device Management* untuk mengontrol akses berdasarkan perangkat pengguna yang dapat dipercaya. Selain itu, terdapat fitur manajemen pengguna khusus *admin*, yang memungkinkan pengelolaan akun secara menyeluruh, termasuk melihat, mengedit, dan menghapus pengguna, serta mengatur hak akses berdasarkan empat peran utama *Student*, *Admin*, *Staff*, dan *General*. Hasil pengujian menunjukkan bahwa implementasi *Zero Trust* berbasis *MFA* berhasil meningkatkan keamanan autentikasi pada *My Petra*, mencegah akses tidak sah, serta memastikan perlindungan data tanpa mengurangi kenyamanan pengguna dalam mengakses sistem.

Kata Kunci: zero trust, multi-factor authentication, LDAP, google oauth, laravel, MFA, autentikasi dua faktor, manajemen pengguna, trusted device.

ABSTRACT

Abiel Nathanael Georgius Pasaribu:

Undergraduate Final Project

Prototype Implementation of Zero Trust Based on Multi-Factor Authentication to Enhance Security in My Petra Application

Protection of academic information systems is very important to prevent data leaks due to cyber-attacks, including repeated login attempts (brute-force), unauthorized access, or the use of default passwords that have not been changed. Petra Christian University has replaced the Single Sign-On (SSO) authentication method with Lightweight Directory Access Protocol (LDAP) to enhance the security of *My Petra* application access. This study develops an authentication system *prototype* based on Zero Trust Architecture (ZTA) with Multi-Factor Authentication (MFA) using *Laravel* as the backend and Blade as the user interface, hosted on cPanel for testing. The system implements OTP (One-Time Password) authentication via Google Authenticator, email, and SMS/Whatsapp, along with Trusted Device Management to regulate access based on user trusted devices. Additionally, a user management feature for administrators is provided, enabling comprehensive account management, including viewing, editing, deleting users, and assigning access rights based on four main roles Student, Admin, Staff, and General. The test results indicate that the implementation of Zero Trust-based MFA successfully enhances authentication security in My Petra, prevents unauthorized access, and ensures data protection without compromising user experience in accessing the system.

Keywords: zero trust, multi-factor authentication, LDAP, google oauth, laravel, MFA, two-factor authentication, user management, trusted device.

DAFTAR ISI

JUDUL	i
LEMBAR PENGESAHAN.....	ii
LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI	iii
LEMBAR DISCLAIMER PENGGUNAAN ARTIFICIAL INTELLIGENCE	iv
KATA PENGANTAR.....	v
ABSTRAK	vi
ABSTRACT	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	xii
DAFTAR TABEL.....	xvi
DAFTAR SEGMENT PROGRAM	xvii
1. PENDAHULUAN	1
1.1. Latar Belakang Permasalahan	1
1.2. Perumusan Masalah.....	2
1.3. Tujuan Tugas Akhir	3
1.4. Manfaat Tugas Akhir	3
1.4.1. Manfaat Praktis	3
1.4.2. Manfaat Akademis	3
1.5. Ruang Lingkup	4
1.6. Metodologi Penelitian.....	6
1.7. Sistematika Penulisan.....	8
2. LANDASAN TEORI	9
2.1. Tinjauan Pustaka	9
2.1.1. Zero Trust	9
2.1.2. Multi-Factor Authentication (MFA).....	10
2.1.3. Lightweight Directory Access Protocol (LDAP).....	10
2.1.4. Two-Factor Authentication (2FA).....	11
2.1.5. Penggunaan Virtual Machine dalam Penerapan Zero Trust berbasis Multi-Factor Authenticator	11
2.1.6. Google Authenticator.....	11

2.1.7. Single Sign-On (SSO).....	12
2.1.8. Laravel dalam My Petra.....	12
2.1.9. User and Device Trust Scoring	13
2.1.10. Zero Trust berbasis MFA	14
2.1.11. Penerapan MFA dalam LDAP	14
2.2. Tinjauan Studi.....	14
2.2.1. Resilient and Optimized LDAP Database Implementation for a Large Scale HLR/HS	14
2.2.2. Implementasi Multi-Factor Authentication pada phpMyAdmin.....	15
2.2.3. Protection Second Layer Menggunakan Multi-Factor Authenticator untuk Memverifikasi Keabsahan Akun Email di Dalam Active Directory	16
2.2.4. Tabel Perbandingan	16
3. ANALISIS DAN DESAIN SISTEM	20
3.1. Analisa Permasalahan	20
3.2. Analisa Pendekatan Tugas Akhir	21
3.3. Analisa Kebutuhan Sistem.....	22
3.3.1. Kebutuhan Fungsionalitas	22
3.3.2. Kebutuhan Non-Fungsionalitas	23
3.4. Diagram Perancangan Sistem	24
3.4.1. Blok Diagram Sistem	24
3.4.2. Use Case Diagram dan Activity Diagram	24
3.4.3. Entity Relationship Diagram (ERD)	26
3.5. Pendekatan Analisis Data	27
3.5.1. Exploratory Data Analysis (EDA).....	27
3.5.2. Sumber Data.....	28
3.5.3. Data Preparation dan Cleansing.....	28
3.6. Flowchart dan Arsitektur Sistem	28
3.6.1. Alur Autentikasi.....	28
3.6.2. Desain Fitur Keamanan	29
3.7. Skenario Pengujian Sistem	35
3.7.1. Tujuan dan Pendekatan Pengujian.....	35
3.7.2. Parameter Pengujian.....	36
3.7.3. Skenario Pengujian	36
3.7.4. Indikator Keberhasilan	36

3.7.5. Pelaporan Hasil.....	37
4. IMPLEMENTASI SISTEM.....	38
4.1. Implementasi sistem	39
4.1.1. Instalasi Laravel.....	39
4.1.2. Instalasi cPanel.....	43
4.2. Implementasi Database.....	46
4.2.1. Pemasangan Database Local.....	46
4.2.2. Pemasangan Google Database.....	61
4.2.3. Pemasangan LDAP Petra	64
4.3. Implementasi Fungsionalitas.....	68
4.3.1. Autentikasi dan Registrasi Pengguna	68
4.3.2. Implementasi Multi-Factor Authentication (MFA).....	72
4.3.3. Pengelolaan Perangkat dan Sesi Login	78
4.3.4. Pembatasan Akses dan Middleware Keamanan	81
4.3.5. Pengelolaan Profil dan Role Sementara.....	84
4.3.6. Sistem Tiket Bantuan dan Notifikasi Email.....	86
4.3.7. Manajemen Admin dan Pengguna.....	89
4.3.8. Viewer Log Sistem	90
4.3.9. Routing dan Validasi Permintaan	91
4.4. Deployment pada Server Production.....	94
5. PENGUJIAN SISTEM	95
5.1. Rencana Pengujian	95
5.2. Metode Pengujian	95
5.3. Hasil Pengujian	96
5.3.1. Pengujian Tampilan dan Fungsionalitas.....	96
5.3.1.1. Tampilan dan Fungsionalitas Autentikasi	96
5.3.1.2. Tampilan dan Fungsionalitas Dashboard	100
5.3.1.3. Tampilan dan Fungsionalitas Profile Setting	104
5.3.1.4. Tampilan dan Fungsionalitas Manage Session Setting	106
5.3.1.5. Tampilan dan Fungsionalitas Security atau MFA Setting	107
5.3.1.6. Tampilan dan Fungsionalitas Manage User Setting	111
5.3.1.7. Tampilan dan Fungsionalitas Passwordless Login.....	113
5.3.1.8. Tampilan dan Fungsionalitas Customer Support	114

5.3.1.9. Tampilan dan Fungsionalitas MFA Challenge	116
5.3.1.10. Tampilan dan Fungsionalitas Device Limit	118
5.3.1.11. Tampilan dan Fungsionalitas Email dan Log Page.....	119
5.3.2. Pengujian Perbandingan dengan My Petra Asli	124
5.3.3. Pengujian Ketahanan terhadap Serangan.....	126
5.3.4. Pengujian Survei Pengguna	132
5.4. Evaluasi Hasil Pengujian Sistem	144
5.4.1. Berdasarkan Tampilan dan Fungsionalitas.....	144
5.4.2. Berdasarkan Penanganan Ancaman	145
5.4.3. Berdasarkan Umpan Balik Pengguna	146
6. KESIMPULAN DAN SARAN	147
6.1. Kesimpulan	147
6.2. Saran.....	148
DAFTAR PUSTAKA.....	149
LAMPIRAN	152

DAFTAR GAMBAR

Gambar 2.1. Zero Trust (Microsoft, 2022)	9
Gambar 3.1. Tahapan Tugas Akhir	21
Gambar 3.2. Arsitektur Prototype My Petra	22
Gambar 3.3. Blok Diagram Prototype My Petra	24
Gambar 3.4. Use Case Diagram Prototype My Petra	25
Gambar 3.5. Activity Diagram Prototype My Petra	26
Gambar 3.6. ERD Prototype My Petra.....	27
Gambar 3.7. Alur Autentikasi Prototype My Petra	29
Gambar 3.8. Alur MFA Prototype My Petra	29
Gambar 3.9. Alur Manage User Prototype My Petra	30
Gambar 3.10. Alur Manage User Device Prototype My Petra	31
Gambar 3.11. Alur Session Prototype My Petra	32
Gambar 3.12. Alur Login Tidak Sah Prototype My Petra	33
Gambar 3.13. Alur External Privacy Control Prototype My Petra.....	33
Gambar 3.14. Alur Passwordless Login Prototype My Petra	34
Gambar 3.15. Alur Pembuatan LDAP Account Prototype My Petra	35
Gambar 4.1. Enviroment Variable.....	40
Gambar 4.2. PHP dan Composer Testing	40
Gambar 4.3. Tampilan Struktur Awal Project Prototype My Petra.....	42
Gambar 4.4. Tampilan Awal Project Prototype My Petra.....	43
Gambar 4.5. Tampilan Awal cPanel	44
Gambar 4.6. Tampilan file Manager cPanel	44
Gambar 4.7. Tampilan Upload file dalam cPanel.....	44
Gambar 4.8. Isi Direktori public_html cPanel	45
Gambar 4.9. Pembuatan Database cPanel untuk Proyek	46
Gambar 4.10. Isi Folder Database Prototype My Petra	47
Gambar 4.11. Isi Folder Models Prototype My Petra	57
Gambar 4.12. Struktur Database pada phpMyAdmin.....	61
Gambar 4.13. Konfigurasi Google Oauth	62
Gambar 4.14. Testing Koneksi LDAP Record	66

Gambar 4.15. Testing Koneksi LDAP Tinker	66
Gambar 5.1. Tampilan Login	97
Gambar 5.2. Tampilan Login Publik.....	98
Gambar 5.3. Tampilan Login Admin.....	98
Gambar 5.4. Tampilan Forgot Your Password	99
Gambar 5.5. Tampilan Register New Account	99
Gambar 5.6. Tampilan Register LDAP Account	100
Gambar 5.7. Tampilan Dashboard Student.....	101
Gambar 5.8. Tampilan Dashboard Staff.....	102
Gambar 5.9. Tampilan Dashboard Admin.....	102
Gambar 5.10. Tampilan Dashboard Publik.....	102
Gambar 5.11. Tampilan Role Switcher.....	103
Gambar 5.12. Tampilan Manage Your Account	103
Gambar 5.13. Tampilan Profile Setting.....	105
Gambar 5.14. Tampilan Setting Page.....	106
Gambar 5.15. Tampilan Session Setting.....	106
Gambar 5.16. Data Session	107
Gambar 5.17. Tampilan Security Setting.....	108
Gambar 5.18. Mobile Authentication Activation	109
Gambar 5.19. Mobile Authentication Scanning.....	109
Gambar 5.20. Tampilan Metode MFA telah Aktif	110
Gambar 5.21. Tampilan Manage Device	110
Gambar 5.22. Tampilan Manage Users.....	112
Gambar 5.23. Tampilan Passwordless Login.....	113
Gambar 5.24. Tampilan Customer Support	114
Gambar 5.25. Tampilan OTP Challenge.....	116
Gambar 5.26. OTP dari WhatsApp	117
Gambar 5.27. OTP dari SMS.....	118
Gambar 5.28. Tampilan Peringatan Maximum OS.....	119
Gambar 5.29. Email untuk OTP	120
Gambar 5.30. Email untuk Passwordless Login.....	121
Gambar 5.31. Email untuk Akses Perangkat Baru.....	121
Gambar 5.32. Email untuk Peringatan Pelanggaran	122

Gambar 5.33. Email untuk Customer Support	122
Gambar 5.34. Email untuk LDAP Account Creation	123
Gambar 5.35. Tampilan Page Log Viewer Admin.....	123
Gambar 5.36. Contoh Log Google Oauth	124
Gambar 5.37. Peringatan Akun Mendapat Banned	127
Gambar 5.38. Kondisi Banned dalam PhpMyAdmin	127
Gambar 5.39. Peringatan Too Many Requests	129
Gambar 5.40. Peringatan Salah Format	131
Gambar 5.40. Survey Tampilan Login	132
Gambar 5.41. Survey Tiga Jalur Login	133
Gambar 5.42. Survey Kemudahan Fitur Forgot Password	133
Gambar 5.43. Survey Kemudahan Fitur Register	133
Gambar 5.44. Survey Kemudahan Fitur Customer Support.....	134
Gambar 5.45. Survey Redireksi ke Dashboard Berdasarkan Role.....	134
Gambar 5.46. Survey Kejelasan Informasi di Dashboard.....	135
Gambar 5.47. Survey Pemahaman Aktivasi MFA.....	135
Gambar 5.48. Survey MFA yang Disukai	136
Gambar 5.49. Survey Kecukupan Metode MFA.....	136
Gambar 5.50. Survey Saran Metode MFA Tambahan.....	137
Gambar 5.51. Survey Kemudahan Login dengan MFA.....	137
Gambar 5.52. Survey Kejelasan Fitur Manage Device	138
Gambar 5.53. Survey Manfaat Pengelolaan Perangkat Login.....	138
Gambar 5.54. Survey Pembatasan Maksimal 3 Perangkat	139
Gambar 5.55. Survey Bantuan Saat Pembatasan Perangkat	139
Gambar 5.56. Survey Manfaat Fitur Manage User bagi Admin	140
Gambar 5.57. Survey Kemudahan Fitur Manage User.....	140
Gambar 5.58. Survey Kecukupan Fitur Pengelolaan Akun.....	140
Gambar 5.59. Survey Kejelasan Pesan Gagal Login atau OTP Salah	141
Gambar 5.60. Survey Bantuan Instruksi Saat Gagal Login/OTP	141
Gambar 5.61. Survey Pemahaman Fitur Passwordless Login	141
Gambar 5.62. Survey Kemudahan Login dengan Passwordless Login	142
Gambar 5.63. Survey Keamanan Passwordless Login dengan MFA	142
Gambar 5.64. Survey Kebermanfaatan Fitur Role Changer	142

Gambar 5.65. Survey Kemudahan Fitur Role Changer143

DAFTAR TABEL

Tabel 2.1. Perbandingan Tinjauan Studi.....	16
Tabel 4.1. Perencanaan Fitur Prototype My Petra.....	38
Tabel 5.1. Rencana Pengujian Sistem.....	95
Tabel 5.2. Perbandingan dengan My Petra Asli	124
Tabel 5.3. Evaluasi Tampilan dan Fungsionalitas	144
Tabel 5.4. Evaluasi Penanganan Ancaman	145
Tabel 5.5. Evaluasi Umpan Balik Pengguna.....	146

DAFTAR SEGMENT PROGRAM

Segmen Program 4.1. Konfigurasi Awal Database Proyek	42
Segmen Program 4.2. Pengubahan Path autoload dan bootstrap dalam cPanel	45
Segmen Program 4.3. Konfigurasi Database Proyek dalam cPanel	46
Segmen program 4.4. UserFactory.php	48
Segmen Program 4.5. create_users_table.php.....	48
Segmen Program 4.6. create_cache_table.php.....	49
Segmen Program 4.7. create_jobs_table.php.....	50
Segmen Program 4.8. add_ldap_columns_to_users_table.php.....	50
Segmen Program 4.9. create_trusted_devices_table.php.....	50
Segmen Program 4.10. add_otp_expires_at_to_users_table.php	51
Segmen Program 4.11. add_passwordless_enabled_to_users_table.php.....	51
Segmen Program 4.12. add_temporary_role_to_users_table.php.....	52
Segmen Program 4.13. create_mfa_table.php	52
Segmen Program 4.14. remove_mfa_columns_from_users_table.php.....	53
Segmen Program 4.15. create_ticketings_table.php.....	54
Segmen Program 4.16. remove_temporary_role_from_users_table.php	54
Segmen Program 4.17. create_roles_and_role_user_tables.php	54
Segmen Program 4.18. RolesTableSeeder.php	55
Segmen Program 4.19. RoleUserSeeder.php	55
Segmen Program 4.20. TrustedDevicesSeeder.php.....	56
Segmen Program 4.21. UserSeeder.php	57
Segmen Program 4.22. Mfa.php	58
Segmen Program 4.23. Role.php.....	58
Segmen Program 4.24. Session.php.....	59
Segmen Program 4.25. Ticketing.php	59
Segmen Program 4.27. User.php	60
Segmen Program 4.26. TrustedDevice.php.....	60
Segmen Program 4.27. Konfigurasi Enviroment Google.....	62
Segmen Program 4.28. Registrasi Enviroment Google	63
Segmen Program 4.29. Pembuatan Rute untuk Penggunaan Google Login.....	63
Segmen Program 4.30. Konfigurasi Enviroment LDAP.....	65

Segmen Program 4.31. Registrasi Enviroment LDAP	65
Segmen Program 4.32. Konfigurasi Rute Autentikasi LDAP	67
Segmen Program 4.33. Kode Proses Login.....	69
Segmen Program 4.34. Kode Register Pengguna.....	70
Segmen Program 4.35. Register LDAP Account	70
Segmen Program 4.36. Kode Alur Login.....	71
Segmen Program 4.37. LDAP Login Route	71
Segmen Program 4.38. Kode Penyimpanan Password	72
Segmen Program 4.39. Kode Reset Password	72
Segmen Program 4.40. Kode Pemilihan Metode MFA.....	73
Segmen Program 4.41. Kode Penyimpanan Metode MFA.....	74
Segmen Program 4.42. Model Metode MFA	74
Segmen Program 4.43. Metode Verifikasi MFA.....	75
Segmen Program 4.44. Check Validasi Verifikasi MFA.....	75
Segmen Program 4.45. Kirim OTP dari Email	76
Segmen Program 4.46. Pemanggilan Email OTP	76
Segmen Program 4.47. Kadarluarsa OTP	76
Segmen Program 4.48. Pemanggilan Magic Link Email Passwordless Login	77
Segmen Program 4.49. Model Tabel MFA	77
Segmen Program 4.50. Konfigurasi Log System dalam Proyek.....	77
Segmen Program 4.51. Check Violation OTP	77
Segmen Program 4.52. Force Logout Violation OTP	77
Segmen Program 4.53. User Model untuk Log System.....	78
Segmen Program 4.54. Kode Hapus Device setelah 30 Hari.....	79
Segmen Program 4.55. Check User Device	79
Segmen Program 4.56. Create Trusted Device	79
Segmen Program 4.57. Model Trusted Device.....	79
Segmen Program 4.58. Validate External OTP	80
Segmen Program 4.59. Validate Logout Violation External OTP	80
Segmen Program 4.60. External OTP Email	80
Segmen Program 4.61. Build External OTP Email	80
Segmen Program 4.62. Ambil Data Sesi	81
Segmen Program 4.63. Hapus Sesi.....	81

Segmen Program 4.64. Hapus Semua Sesi	81
Segmen Program 4.65. Check MFA Redirect	82
Segmen Program 4.66. Check Active Role	82
Segmen Program 4.67. Check Banned User	83
Segmen Program 4.68. Redirect MFA Challenge Page.....	83
Segmen Program 4.69. Konfigurasi Rate Limiting	83
Segmen Program 4.70. Pengecekan Role Aktif	83
Segmen Program 4.71. Role Aktif dalam Session.....	84
Segmen Program 4.72. Kode Pembatasan Akses.....	85
Segmen Program 4.73. Relasi Table Roles dan Table Users.....	85
Segmen Program 4.74. Relasi Table Users dan Table Roles.....	85
Segmen Program 4.75. Validasi Tabel MFA	85
Segmen Program 4.76. Konfigurasi Table Users	86
Segmen Program 4.77. Perbaruan Tabel Users dan MFA	86
Segmen Program 4.78. Pembuatan Data Ticketing Baru	87
Segmen Program 4.79. Pengiriman Ticketing Baru.....	88
Segmen Program 4.80. Pelaporan Ticketing Baru.....	88
Segmen Program 4.81. Pengiriman Ticketing Baru lewat WhatsApp	88
Segmen Program 4.82. Pengiriman Email Violation kepada Admin	89
Segmen Program 4.83. Contoh Update Data User	90
Segmen Program 4.84. Log Perubahan Data User	90
Segmen Program 4.85. Penampilan Page Manage User.....	90
Segmen Program 4.86. Contoh Log yang Ditampilkan.....	91
Segmen Program 4.87. Pengaturan Log Viewer untuk Admin.....	91
Segmen Program 4.88. Pemisahan Rute untuk Berbagai Role	92
Segmen Program 4.89. Kumpulan Middleware dalam Routes	93
Segmen Program 5.1. Kode Testing DDOS.....	128