

## DAFTAR ISI

**LEMBAR PERSETUJUAN**

**LEMBAR PENGESAHAN**

**SURAT PERNYATAAN KARYA SENDIRI**

**ABSTRAK.....I**

**ABSTRACT .....II**

**KATA PENGANTAR.....III**

**DAFTAR ISI.....V**

**DAFTAR GAMBAR.....VII**

**DAFTAR TABEL.....VIII**

**BAB I PENDAHULUAN.....1**

1.1	LATAR BELAKANG .....	1
1.2	PERUMUSAN MASALAH .....	3
1.3	TUJUAN PENELITIAN .....	4
1.4	MANFAAT PENELITIAN.....	4
1.5	BATASAN MASALAH .....	4
1.6	KERANGKA PEMIKIRAN .....	5
1.7	METODOLOGI PENGERJAAN TUGAS AKHIR .....	7
1.7.1	<i>Metode Pengumpulan Data</i> .....	7
1.8	SISTEMATIKA PENULISAN .....	9

**BAB II STUDI PUSTAKA.....11**

2.1	TINJAUAN PUSTAKA.....	11
2.1.1	<i>The state of the art</i> .....	11
2.2	LANDASAN TEORI .....	13
2.2.1	<i>Website</i> .....	13
2.2.1.1	<i>Web Statis</i> .....	14
2.2.1.2	<i>Web Dinamis</i> .....	14
2.2.2	<i>Microservice Architecture</i> .....	15
2.2.3	<i>JSON Web Token (JWT)</i> .....	15
2.2.4	<i>Pengertian Kriptografi</i> .....	17
2.2.5	<i>Advanced Encryption Standards (AES)</i> .....	20
2.2.6	<i>Struktur Proses Enkripsi AES 128 bit</i> .....	21
2.2.7	<i>Struktur Proses Dekripsi AES 128 bit</i> .....	22
2.2.8	<i>Transformasi – transformasi pada algoritma AES</i> .....	23
2.2.9	<i>Model Prototyping</i> .....	28
2.3	APLIKASI PENDUKUNG.....	30
2.3.1	<i>Pemograman PHP</i> .....	30
2.3.2	<i>MySQL</i> .....	31
2.3.3	<i>Laravel Framework</i> .....	31
2.3.4	<i>UML</i> .....	32
2.3.5	<i>Use Case Diagram</i> .....	33
2.3.6	<i>Activity Diagram</i> .....	34

**BAB III ANALISIS DAN PERANCANGAN.....35**

3.1	ANALISIS SISTEM .....	35
3.2	ANALISIS KEBUTUHAN.....	36

3.2.1	<i>Pemodelan Kebutuhan Sistem</i>	36
3.2.2	<i>Kebutuhan Perangkat Keras (Hardware)</i>	38
3.2.3	<i>Kebutuhan Perangkat Lunak (Software)</i>	38
3.2.4	<i>Pengguna (Brainware)</i>	38
3.2.5	<i>Analisis Algoritma AES (Advanced Encryption Standard)</i>	39
3.2.6	<i>Analisis JSON Web Token (JWT)</i>	46
3.3	PERANCANGAN SISTEM	48
3.3.1	<i>Arsitektur Sistem Usulan</i>	48
3.3.2	<i>Use Case Diagram</i>	50
3.3.3	<i>Activity Diagram</i>	55
3.3.4	<i>Prototype Layanan Autentikasi (API Spec)</i>	56
<b>BAB IV IMPLEMENTASI DAN PENGUJIAN</b>		<b>68</b>
4.1	IMPLEMENTASI	68
4.2	IMPLEMENTASI PERANGKAT KERAS	68
4.3	TUJUAN IMPLEMENTASI PERANGKAT LUNAK	68
4.4	IMPLEMENTASI ALGORITMA	69
4.4.1	<i>Enkripsi AES-128</i>	69
4.4.2	<i>Dekripsi AES-128</i>	72
4.4.3	<i>Implementasi JWT</i>	75
4.5	IMPLEMENTASI DAN PENGUJIAN API	77
4.5.1	<i>Login Endpoint</i>	79
4.5.2	<i>Refresh Token Endpoint</i>	80
4.5.3	<i>Logout Endpoint</i>	81
4.5.4	<i>Update Device Id</i>	81
4.5.5	<i>Data Bantuan</i>	82
4.5.6	<i>Masukan Bantuan</i>	82
4.5.7	<i>Data Fitur Aplikasi</i>	82
4.5.8	<i>Data Halaman Utama</i>	82
4.5.9	<i>Data Banner Halaman Utama</i>	83
4.5.10	<i>Data Custom Text Aplikasi</i>	84
4.5.11	<i>Data Popup Iklan</i>	84
4.5.12	<i>Data Informasi Aplikasi</i>	84
4.5.13	<i>Masukan Pengguna</i>	85
4.5.14	<i>Generate Deeplink</i>	86
4.5.15	<i>Data Kontak Admin</i>	87
4.5.16	<i>Simpan Kontak Admin</i>	87
4.5.17	<i>Data Device Id</i>	87
4.5.18	<i>Data Pengguna</i>	88
4.5.19	<i>Cari Pengguna</i>	88
4.5.20	<i>Update Data Pengguna</i>	89
4.5.21	<i>Update Foto Profil</i>	90
4.6	PENGUJIAN BLACK BOX	91
4.6.1	<i>Pengujian Proses Enkripsi algoritma AES-128</i>	91
4.6.2	<i>Pengujian API</i>	93
4.6.3	<i>Pengujian Algoritma</i>	94
<b>BAB V PENUTUP</b>		<b>99</b>
5.1	KESIMPULAN	99
5.2	SARAN	99
<b>DAFTAR PUSTAKA</b>		<b>101</b>
<b>LAMPIRAN</b>		<b>102</b>

## DAFTAR GAMBAR

Gambar 1.1 Skema Kerangka Pemikiran.....	6
<i>Gambar 1.2 Arsitektur Prototype .....</i>	8
Gambar 2.1 Contoh JSON Web Token .....	16
Gambar 2.2 Contoh hasil dari proses verifikasi JSON Web Token .....	16
Gambar 2.3 Skema Proses Kriptografi .....	19
Gambar 2.4 Skema Enkripsi AES 128 bit [6].....	22
Gambar 2.5 Skema dekripsi AES 128 bit [7] .....	23
Gambar 2.6 Skema Transformasi ShiftRows .....	25
Gambar 2.7 Inverse ShiftRows.....	27
Gambar 2.8 Model Prototype [11].....	30
Gambar 3.1 Tabel S-Box .....	40
Gambar 3.2 Bagian <i>Header</i> dari JWT .....	47
Gambar 3.3 Bagian <i>Payload</i> dari JWT .....	47
Gambar 3.4 Bagian <i>Signature</i> dari JWT.....	48
Gambar 3.5 Arsitektur Sistem .....	49
Gambar 3.6 Alur sistem kriptografi yang akan dirancang.....	49
Gambar 3.7 Use case diagram sistem yang dibangun .....	50
Gambar 3.8 Activity diagram login .....	55
Gambar 3.9 Activity diagram logout dan refresh token .....	56
Gambar 4.1 Uji Performa Enkripsi dan Dekripsi .....	94
Gambar 4.2 Selisih waktu dari enkripsi dan dekripsi .....	95
Gambar 4.3 Hasil monitoring jaringan menggunakan HTTP Analyzer .....	96
Gambar 4.4 Detail dari hasil monitoring jaringan .....	97



## DAFTAR TABEL

Tabel 2.1 State of The Art .....	11
Tabel 2.2 Hubungan Panjang key AES dan jumlah round key .....	21
Tabel 2.3 S-BOX [5].....	24
Tabel 2.4 Tabel inverse S-BOX.....	27
Tabel 2.5 Simbol – simbol use case diagram.....	33
Tabel 2.6 Simbol – simbol Activity Diagram.....	34
Tabel 3.1 Functional Requirements .....	36
Tabel 3.2 Tabel matriks polynomial .....	44
Tabel 3.3 Actor .....	51
Tabel 3.4 Definisi Use Case .....	51
Tabel 3.5 Skenario use case login.....	52
Tabel 3.6 Skenario use case register.....	52
Tabel 3.7 Skenario use case refresh token.....	52
Tabel 3.8 Skenario use case get user info .....	53
Tabel 3.9 Skenario use case update user info .....	53
Tabel 3.10 Skenario use case logout.....	54
Tabel 3.11 Skenario use case get secured resources.....	54
Tabel 3.12 Skenario use case get unsecured resources.....	54
Tabel 4.1 Spesifikasi perangkat keras (hardware) .....	68
Tabel 4.2 Spesifikasi perangkat lunak (software).....	68
Tabel 4.3 Tabel endpoint sistem .....	77
Tabel 4.4 Hasil decode JWT .....	92
Tabel 4.5 Pengujian API.....	93

