

100/FKOM-UNIKU/SKRIPSI/XII/2025

**IMPLEMENTASI KEAMANAN KOMUNIKASI DATA BERBASIS REST
API WEB SERVICE DENGAN PENERAPAN KRIPTOGRAFI ADVANCED
ENCRYPTION STANDARD**

(Studi Kasus: Aplikasi Android gurungaji.com PT. Bakti Indonesia Mengaji)

SKRIPSI

Diajukan Untuk Memenuhi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer Program Studi Teknik Informatika



Oleh:

MUHAMMAD AKBAR NUGRAHA

20190810082

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS KUNINGAN

2025

LEMBAR PENGESAHAN

IMPLEMENTASI KEAMANAN KOMUNIKASI DATA BERBASIS RESTAPI WEB SERVICE DENGAN PENERAPAN KRIPTOGRAFI ADVANCED ENCRYPTION STANDARD

(Studi Kasus: Aplikasi Android gurungaji.com PT. Bakti Indonesia Mengaji)

Disusun Oleh :

Muhammad Akbar Nugraha

20190810082

Program Studi Teknik Informatika Jenjang S1

Skripsi ini telah dibimbingkan kepada para pembimbing sesuai dengan SK bimbingan Skripsi/Tugas Akhir di Program Studi Teknik Informatika Jenjang S1 Fakultas Ilmu Komputer Univesitas Kuningan dan telah disetujui pada :

Tempat : Fakultas Ilmu Komputer

Hari : Kamis

Tanggal Bulan Tahun : 13 Juni 2024

DOSEN PEMBIMBING :

Pembimbing 1



Yati Nurhayati, M. Kom
NIK. 41038091290

Pembimbing 2



Fitra Nugraha, M. Kom
NIK. 41038111389

Mengetahui / Mengesahkan :
Kepala Program Studi Teknik Informatika



Yati Nurhayati, M. Kom
NIK. 41038091290

LEMBAR PENGUJIAN

IMPLEMENTASI KEAMANAN KOMUNIKASI DATA BERBASIS REST API WEB SERVICE DENGAN PENERAPAN KRIPTOGRAFI ADVANCED ENCRYPTION STANDARD

(Studi Kasus: Aplikasi Android gurungaji.com PT. Bakti Indonesia Mengaji)

Disusun Oleh :

Muhammad Akbar Nugraha

20190810082

Program Studi Teknik Informatika Jenjang S1

Skripsi ini telah diajukan dan Dipertahankan di Depan Dosen Penguji Sidang Skripsi, Program Studi Teknik Informatika Jenjang S1 Fakultas Komputer Universitas Kuningan dan telah disetujui pada :

Tempat : Fakultas Ilmu Komputer

Hari : Kamis

Tanggal Bulan Tahun : 13 Juni 2024

DOSEN PENGUJI :

Penguji I



Rio Priantama, M.T.I
NIK. 41038101346

Penguji II



Siti Maesyaroh, M.Kom
NIK. 41038111387

Penguji III



Fitra Nugraha, M.Kom
NIK. 41038111389

Mengetahui/Mengesahkan



Dekan
Fakultas Ilmu Komputer

Tito Sugiharto, S.Kom., M.Eng
NIK. 41038101348

Kepala Program Studi
Teknik Informatika S1


Yati Nurhayati, M. Kom
NIK. 41038091290

SURAT PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : Muhammad Akbar Nugraha

NIM : 20190810082

Tempat, Tanggal lahir : Cirebon, 24 Mei 2001

Program Studi : Teknik Informatika

Fakultas : Ilmu Komputer

Perguruan Tinggi : Universitas Kuningan

Menyatakan bahwa **Skripsi** dengan judul sebagai berikut :

Judul : **IMPLEMENTASI KEAMANAN KOMUNIKASI DATA BERBASIS REST API WEB SERVICE DENGAN PENERAPAN KRIPTOGRAFI ADVANCED ENCRYPTION STANDARD (Studi Kasus : Aplikasi Android gurungaji.com PT. Bakti Indonesia Mengaji)**

Dosen Pembimbing 1 : Yati Nurhayati, M.Kom.

Dosen Pembimbing 2 : Fitra Nugraha, M.Kom.

Adalah benar benar **ASLI** dan **BUKAN PLAGIAT** yakni tidak melakukan penjiplakan pada karya tulis ilmiah milik orang lain, kecuali yang dikembangkan dan diacu dalam daftar pustaka pada Skripsi / Tugas Akhir ini.

Demikian pernyataan ini **SAYA** buat, apabila kemudian hari terbukti **SAYA** melakukan penjiplakan karya orang lain, maka **SAYA** bersedia menerima **SANKSI AKADEMIK**.

Kuningan, 13 Juni 2024

Yang menyatakan,

A handwritten signature in black ink is written over a yellow postage stamp. The stamp features the Garuda Pancasila emblem and the text '1000', 'METERAI TEMPEL', and '315DEAMX326411480'.

Muhammad Akbar Nugraha

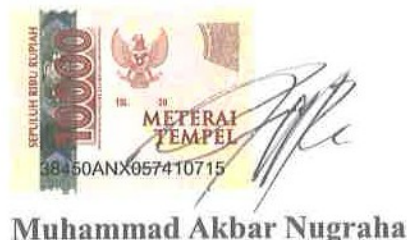
PERNYATAAN ORIGINALITAS

Bismillahirrahmanirrahim

Dengan ini saya menyatakan bahwa skripsi yang berjudul **IMPLEMENTASI KEAMANAN KOMUNIKASI DATA BERBASIS REST API WEB SERVICE DENGAN PENERAPAN KRIPTOGRAFI ADVANCED ENCRYPTION STANDARD (Studi Kasus : Aplikasi Android gurungaji.com PT. Bakti Indonesia Mengaji)** beserta seluruh isinya adalah benar karya saya sendiri dan saya tidak melakukan penjiplakan atau pengutipan dengan cara yang tidak sesuai dengan etika yang berlaku dalam masyarakat keilmuan.

Atas dasar pernyataan ini saya siap menanggung resiko atau sanksi apa pun yang sesuai dengan peraturan yang berlaku apabila di kemudian hari ditemukan adanya pelanggaran terhadap etika keilmuan atau ada klaim dari pihak lain terhadap keaslian skripsi ini.

Kuningan, 13 Juni 2024
Yang membuat pernyataan,



Muhammad Akbar Nugraha

MOTTO

“Buat tujuan yang jelas, buat sesuatu hal menjadi menarik, buat kebiasaan menjadi mudah, dan buat suatu hal menjadi memuaskan.”

PERSEMBAHAN

Skripsi ini saya persembahkan untuk :

1. Orang tua yang senantiasa memberikan *support* ,dan mengupayakan segala hal demi pendidikan dan kehidupan.
2. Bapak Laurensius Dede Suhardiman dan Bapak Gusti Tria Nurcahya yang selalu memberikan *support*, nasihat, dan berbagi ilmu untuk terus berkembang tanpa memandang apapun.
3. Hana Ayu Pratiwi yang telah membantu meminjamkan laptopnya untuk keberlangsungan naskah skripsi saya.
4. Jamaah Balong yang selalu memberikan *support* tanpa batas untuk menyelesaikan skripsi saya.
5. Dan semua sahabat, teman-teman yang telah menjadi inspirasi dalam mengerjakan skripsi.

IMPLEMENTASI KEAMANAN KOMUNIKASI DATA BERBASIS REST API WEB SERVICE DENGAN PENERAPAN KRIPTOGRAFI ADVANCED ENCRYPTION STANDARD

(Studi Kasus: Aplikasi Android gurungaji.com PT. Bakti Indonesia Mengaji)

Muhammad Akbar Nugraha¹⁾, Yati Nurhayati²⁾, Fitra Nugraha³⁾

^{1,2,3}Fakultas Ilmu Komputer, Universitas Kuningan

Jl. Pramuka No.67, Purwawinangun, Kec. Kuningan, Kabupaten Kuningan, Jawa Barat 45512

[^{1\)}20190810082@uniku.ac.id](mailto:20190810082@uniku.ac.id), [^{2\)}yati.nurhayati@uniku.ac.id](mailto:yati.nurhayati@uniku.ac.id),
[^{3\)}EmailDosen2@uniku.ac.id](mailto:EmailDosen2@uniku.ac.id)

Abstrak

API atau dikenal dengan *Application Programming Interface* merupakan sebuah pertukaran informasi antara dua atau lebih aplikasi di perangkat lunak. PT. Bakti Indonesia Mengaji adalah sebuah perusahaan yang bergerak di bidang teknologi informasi yang fokus di bidang pembelajaran baca Qur'an. Perusahaan tersebut memiliki sebuah produk aplikasi yang bernama gurungaji.com dan telah terjadi penyerangan secara berulang kali dengan menggunakan metode *SQL Injection* bertujuan untuk mengubah status pembayaran. Penyerangan ini berfokus pada autentikasi *header request* yang tidak memiliki metode enkripsi khusus. Dalam hal ini dilakukan sebuah pengamanan dengan menggunakan Kriptografi *Advanced Encryption Standard 128*, yakni menggunakan kunci yang sama saat melakukan proses enkripsi dan dekripsi pada setiap bit, jumlah *round* terdiri dari 10 putaran pada proses enkripsi dan dekripsi. Proses enkripsi terdiri dari *AddRoundKey*, *SubBytes*, *Shiftrows*, dan *MixColumns*. Proses dekripsi terdiri dari *InvShiftrows*, *InvSubBytes*, *InvMixColumns*, dan *AddRoundKey*. Dalam penelitian ini metodologi perangkat lunak yang digunakan adalah *Rational Unified Process*. Tahap pertama yang dilakukan yaitu *Inception*, dengan melakukan identifikasi melalui pengumpulan data. Tahap kedua yaitu *Elaboration*, dengan melakukan analisis dan desain sistem dengan menggunakan *Unified Modelling Language*. Tahap ketiga yaitu *Construction*, dengan mengimplementasikan kriptografi pada sebuah fitur. Tahap keempat yaitu *Transition*, berupa pengujian sistem. Hasil dari penelitian ini berupa kriptografi *Advanced Encryption Standard 128* dapat diterapkan pada API.

Kata Kunci : *Application Programming Interface; gurungaji.com; Kriptografi; Advanced Encryption Standard 128; Unified Modelling Language; SQL Injection;*

IMPLEMENTATION OF DATA COMMUNICATION SECURITY BASED ON REST API WEB SERVICE WITH THE APPLICATION OF ADVANCED ENCRYPTION STANDARD CRYPTOGRAPHY

(Case Study: Android Application gurungaji.com PT. Bakti Indonesia Mengaji)

Muhammad Akbar Nugraha¹⁾, Yati Nurhayati²⁾, Fitra Nugraha³⁾

^{1,2}, Faculty of Computer Science, University Kuningan

Jl. Pramuka No.67, Purwawinangun, Kec. Kuningan, Kuningan Regency, West Java 45512

[^{1\)}20190810082@uniku.ac.id](mailto:20190810082@uniku.ac.id), [^{2\)}yati.nurhayati@uniku.ac.id](mailto:yati.nurhayati@uniku.ac.id),
[^{3\)}EmailDosen2@uniku.ac.id](mailto:EmailDosen2@uniku.ac.id)

Abstract

An API, or Application Programming Interface, is an exchange of information between two or more software applications. PT. Bakti Indonesia Mengaji is a company operating in the information technology sector, focusing on teaching people to read the Qur'an. The company has an application product called gurungaji.com, which has been repeatedly targeted by SQL Injection attacks aimed at changing payment statuses. These attacks focus on authenticating request headers that do not use a specific encryption method. In response, security is enhanced using Advanced Encryption Standard (AES) 128 cryptography, which employs the same key for both encryption and decryption processes. Each process involves 10 rounds. The encryption process includes AddRoundKey, SubBytes, ShiftRows, and MixColumns. The decryption process consists of InvShiftRows, InvSubBytes, InvMixColumns, and AddRoundKey. This research adopts the Rational Unified Process software methodology. The first stage is Inception, involving identification through data collection. The second stage is Elaboration, where the system is analyzed and designed using Unified Modeling Language. The third stage is Construction, which involves implementing cryptography on a feature. The fourth stage is Transition, which includes system testing. The results of this research demonstrate that Advanced Encryption Standard (AES) 128 cryptography can be successfully applied to APIs.

Keywordsi : Application Programming Interface; gurungaji.com; Kriptografi; Advanced Encryption Standard 128; Unified Modelling Language; SQL Injection;

KATA PENGANTAR

Puji serta syukur Alhamdulillah penulis panjatkan kehadiran Allah SWT yang telah melimpahkan rahmat, hidayat, taufik dan kekuatan sehingga penulis dapat menyelesaikan penyusunan skripsi ini dengan judul **“Implementasi Keamanan Komunikasi Data Berbasis Rest Api Web Service dengan Penerapan Kriptografi Advanced Encryption Standard (Studi Kasus: Aplikasi Android gurungaji.com PT. Bakti Indonesia Mengaji)”**.

Terselesaikannya skripsi ini tidak lepas dari masukan, arahan, dorongan, dukungan serta bimbingan yang diberikan dari berbagai pihak. Dengan kerendahan hati, penulis ingin menyampaikan ucapan terima kasih dan penghargaan sebesar-besarnya kepada :

1. Bapak Dr. H. Dikdik Harjadi, M.Si, selaku Rektor Universitas Kuningan.
2. Bapak Tito Sugiharto, S.Kom, M.Eng. selaku Dekan Fakultas Ilmu Komputer Universitas Kuningan.
3. Ibu Yati Nurhayati, M. Kom, selaku Kepala Program Studi Teknik Informatika S1 Fakultas Ilmu Komputer Universitas Kuningan dan sekaligus Pembimbing I yang sudah banyak meluangkan waktunya untuk membimbing peneliti.
4. Bapak Fitra Nugraha, M. Kom, selaku Pembimbing II yang sudah banyak meluangkan waktunya untuk membimbing peneliti.
5. Bapak dan Ibu Dosen Program Studi Teknik Informatika Fakultas Komputer Universitas Kuningan yang terlag membekali ilmu pengetahuan kepada penulis selama mengikuti perkuliahan.

6. Seluruh Karyawan Tata Usaha dan Program Studi Teknik Informatika Fakultas Komputer Universitas Kuningan atas bantuan dan kerjasamanya.
7. Bapak Laurensius Dede Suhardiman, selaku CTO gurungaji.com yang sudah memberikan izin untuk melakukan penelitian.
8. Orang tua, kakak, dan adik yang telah memberikan do'a, arahan dan dukungan baik material maupun moral.
9. Rekan-rekan KOMITE (Komunitas IT *Enthusiast*) yang telah memberikan arahan dan dukungan baik material maupun moral.
10. Rekan-rekan Mahasiswa Fakultas Ilmu Komputer Universitas Kuningan.
11. Serta semua pihak yang tidak dapat disebutkan satu per satu yang telah memberikan dukungan dan membantu dalam penyelesaian skripsi ini.

Semoga skripsi ini dapat bermanfaat bagi peneliti, tempat/objek penelitian, Institusi dan bagi para pembaca pada umumnya. Atas dukungan dan bantuannya, peneliti mengucapkan banyak terimakasih.

Kuningan, 13 Juni 2024

Peneliti

DAFTAR ISI

LEMBAR PENGESAHAN

LEMBAR PENGUJIAN

SURAT PERNYATAAN

PERNYATAAN ORIGINALITAS

MOTTO dan PERSEMBAHAN

ABSTRAK i

KATA PENGANTAR iii

DAFTAR ISI v

DAFTAR GAMBAR..... viii

DAFTAR TABEL ix

BAB 1 PENDAHULUAN 1

1.1 Latar Belakang 1

1.2 Identifikasi Masalah..... 3

1.3 Rumusan Masalah..... 4

1.4 Batasan Masalah 4

1.5 Tujuan Penelitian 5

1.6 Manfaat Penelitian 5

1.7 Pertanyaan Penelitian..... 6

1.8 Hipotesis Penelitian..... 6

1.9 Metodologi Penelitian..... 7

1.9.1 Metode Pengumpulan Data 7

1.9.2 Metode Pengembangan Sistem..... 9

1.9.3 Metode Penyelesaian Masalah 11

1.10 Jadwal Penelitian 14

1.11 - Sistematika Penelitian..... 15

BAB II LANDASAN TEORI..... 17

2.1 Landasan Teori 17

2.1.1 Representational State Transfer (REST) 17

2.1.2	<i>Application Programming Interface (API)</i>	18
2.1.3	<i>Web Service</i>	18
2.1.4	Komunikasi Data	19
2.1.5	Keamanan Data.....	20
2.1.6	Algoritma Advanced Encryption Standard (AES).....	20
2.1.6.1	Proses Pembangkitan Sub Kunci (<i>Key Schedule</i>).....	21
2.1.6.2	Proses Enkripsi	24
2.1.6.3	Proses Dekripsi	27
2.1.7	Perancangan Sistem.....	38
2.1.7.1	Flowchart	38
2.1.7.2	<i>Unified Modelling Language (UML)</i>	40
2.1.8	Bahasa Pemrograman	46
2.1.8.1	PHP:Hypertext Preprocessor	47
2.1.9	Tools Pendukung	47
2.1.9.1	Apache Web Server.....	47
2.1.9.2	MySQL Database	48
2.1.9.3	Visual Studio Code	48
2.1.9.4	Postman.....	49
2.1.9.5	Draw.io	49
2.1.10	Pengujian Perangkat Lunak	50
2.1.10.1	White Box Testing	50
2.1.10.2	Black Box Testing	51
2.2	Penelitian Sebelumnya.....	51
2.3	Kerangka Teoritis.....	55
BAB III ANALISIS DAN PERANCANGAN		58
3.1	Analisis Sistem (System Analysis)	58
3.1.1	Analisis Masalah	58
3.1.2	Analisis Kebutuhan Fungsional.....	61
3.1.3	Analisis Kebutuhan Non-Fungsional.....	61
3.1.4	Analisis Sistem yang Sedang Berjalan	62
3.1.5	Analisis Sistem Usulan.....	62
3.2	Analisis Algoritma Advanced Encryption Standard (AES)	63

3.2.1	Proses Pembangkitan Sub Kunci.....	64
3.2.2	Proses Enkripsi	68
3.2.3	Proses Dekripsi	75
3.3	Perancangan Sistem (System Design)	81
3.3.1	Use Case Diagram	81
3.3.2	Skenario	82
3.3.3	Activity Diagram	83
3.3.4	Class Diagram	83
3.3.5	Sequence Diagram.....	85
BAB IV	IMPLEMENTASI DAN PENGUJIAN	86
1.1	Implementasi (Implementation)	86
1.2	Perangkat Implementasi	86
1.2.1	Kebutuhan Perangkat Lunak	86
1.2.2	Kebutuhan Perangkat Keras	87
1.3	Pengujian Sistem (<i>System Testing</i>)	87
1.3.1	Pengujian Keamanan	87
1.3.1.1	Enkripsi Key Value.....	87
1.3.1.2	Autentikasi Transaksi dan Dekripsi Key Value	88
1.3.1.3	Autentikasi <i>Header Key Value</i>	90
1.3.2	<i>Black Box Testing</i>	92
1.3.3	<i>White Box Testing</i>	93
1.3.3.1	Enkripsi.....	93
1.3.3.2	Dekripsi	95
BAB V	SIMPULAN DAN SARAN	99
5.1	Simpulan (<i>Conclusion</i>)	99
5.2	Saran (<i>Suggestion</i>)	99
DAFTAR PUSTAKA.....		100
LAMPIRAN		107

DAFTAR GAMBAR

Gambar 1. 1 Metode RUP	10
Gambar 1. 2 FlowChart Enkripsi AES	12
Gambar 1. 3 FlowChart Dekripsi AES	13
Gambar 2. 1 FlowChart Enkripsi AES	25
Gambar 2. 2 Transformasi ShiftRows	26
Gambar 2. 3 Persamaan Transformasi MixColumns	27
Gambar 2. 4 Perkalian Matriks MixColumns	27
Gambar 2. 5 FlowChart Dekripsi AES	28
Gambar 2. 6 Transformasi InvShiftRows	28
Gambar 2. 7 Persamaan Transformasi InvMixColumns	29
Gambar 2. 8 Kerangka Teoritis	55
Gambar 3. 1 Rich Picture Sistem yang sedang berjalan	62
Gambar 3. 2 Rich Picture Sistem yang diusulkan	63
Gambar 3. 3 FlowChart Enkripsi AES	69
Gambar 3. 4 FlowChart Dekripsi AES	75
Gambar 3. 5 Use Case Diagram Sistem	81
Gambar 3. 6 Activity HTTP Request	83
Gambar 3. 7 Class Diagram Transaksi	84
Gambar 3. 8 Sequence Transaksi	85

DAFTAR TABEL

Tabel 1. 2 Jadwal Kegiatan.....	14
Tabel 2. 2 Tabel ASCII	22
Tabel 2. 3 Tabel S-Box	23
Tabel 2. 4 Tabel R-Con.....	23
Tabel 2. 6 Simbol-Simbol FlowChart.....	39
Tabel 2. 7 Simbol-Simbol Usecase.....	41
Tabel 2. 8 Simbol-Simbol Activity	43
Tabel 2. 9 Simbol-Simbol Class Diagram	44
Tabel 2. 10 Simbol-Simbol Sequence.....	45
Tabel 2. 11 Penelitian Sebelumnya.....	52
Tabel 3. 6 tabel SubKunci.....	68
Tabel 3. 7 Proses Perhitungan Enkripsi	73
Tabel 3. 8 Proses Perhitungan Dekripsi.....	79
Tabel 3. 9 Skenario Transaksi.....	82