PERANCANGAN KEAMANAN KOMUNIKASI DATA PADA *REST-API* MENGGUNAKAN ALGORITMA RIJNDEAL

SKRIPSI

Disusun oleh

Ade Kurnianto Santoso

15.61.0057

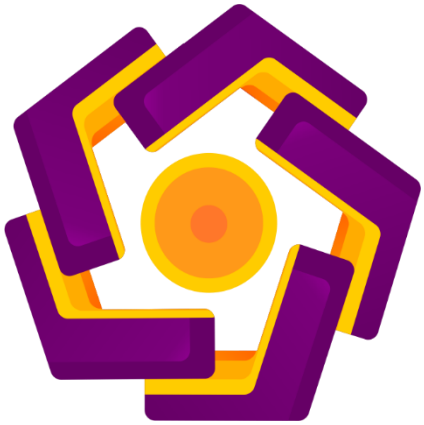
PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA

2021

PERANCANGAN KEAMANAN KOMUNIKASI DATA PADA *REST-API* MENGGUNAKAN ALGORITMA RIJNDEAL

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai derjat Sarjana S1
pada Program Studi Informatika



Disusun oleh
Ade Kurnianto Santoso
15.61.0057

PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2021

PERSETUJUAN

SKRIPSI

PERANCANGAN KEAMANAN KOMUNIKASI DATA PADA *REST-API* MENGGUNAKAN ALGORITMA RIJNDEAL

yang dipersiapkan dan disusun oleh

Ade Kurnianto Santoso

15.61.0057

telah disetujui oleh Dosen Pembimbing Skripsi

pada tanggal 05 Oktober 2021

Dosen Pembimbing,

Joko Dwi Santoso, M.Kom
NIK. 190302181

PENGESAHAN

SKRIPSI

PERANCANGAN KEAMANAN KOMUNIKASI DATA PADA *REST-API* MENGGUNAKAN ALGORITMA RIJNDEAL

yang dipersiapkan dan disusun oleh

Ade Kurnianto Santoso

15.61.0057

telah dipertahankan di depan Dewan Penguji
pada tanggal 19 Oktober 2021

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Mulia Sulistiyono, M.kom. **NIK. 190302248**	_____
Pramudhita Ferdiansyah, M.kom. **NIK. 190302409**	_____
Ria Andriani, M.kom. **NIK. 190302458**	_____

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 19 Oktober 2021

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta, M.Kom
NIK. 190302096

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 19 Oktober 2021

Ade Kurnianto Santoso

NIM. 15.61.0057

MOTTO

“JANGAN MENYOMBONGKAN APA YANG TIDAK KAMU BISA ATAU PUNYA”

“TENTUKAN HIDUPMU SENDIRI BUKAN DI TENTUKAN ORANG LAIN”

Punggung pisaupun bila diasah akan menjadi tajam.

PERSEMBAHAN

Sujud syukur ku persembahkan pada ALLAH yang maha kuasa, berkat dan rahamat detak jantung, denyut nadi, nafas dan putaran roda kehidupan yang diberikan-Nya hinga saat ini saya dapat mempersembahkan skripsi ku pada orang-orang tersayang:

1. Kedua orang tua ku yang sangat kusayang dan kucintai sejak aku belum dilahirkan.
2. Monitor dan Laptop SNSV yang senantiasi menemani 24/7 365 hari
3. (anti shutdown shutdown club)
4. Teruntuk akal dan pikiran ku yang udah try-hard siang malam.
5. Kepada Raka PW dan Mukhlis PA selamat kalian pasangan yang baik.
6. Kepada Bpk. Joko Dwi Santoso terimkasih banyak atas dukungan moril serta nasihatnya.
7. Terimakasih banyak kepada barisan para *mantan* atas dukungan nya selama ini.
8. Buat kamu. Iya kamu yang baca I love u ya.
9. Buat kalian para sahabatku yang ku saying dank u cinta terimakasih ya
10. Khususnya Ipank orang yang paling berperan di dalam hirup ku
11. buat timbul,panjul dan udin terimakasih semangat dan ketawa nya

KATA PENGANTAR

اَلسَّلَامُ عَلَيْكُمْ وَ رَحْمَةُ اللّٰهِ وَبَرَكَاتُهُ

Segala puji dan syukur kami ucapkan kehadirat Allah SWT, Tuhan Yang Maha Esa, Maha Pengasih lagi Maha Penyayang. Sholawat serta salam tidak lupa kami ucapkan kepada Nabi Besar, Muhammad SAW.
Alhamdulillahirabbil'alamin, peneliti dapat menyelesaikan skripsi ini sebagai syarat untuk menamatkan gelar Sarjana (S-1) di Jurusan Teknik Informatika, Universitas AMIKOM Yogyakarta.

Proses penelitian dan penulisan skripsi ini tentu tidak terlepas dari banyaknya pihak yang memberikan bantuan sehingga skripsi ini dapat terselesaikan. Tidak lupa, peneliti juga mengucapkan banyak terima kasih untuk semua pihak yang terlibat secara langsung maupun tidak dalam proses pengerjaan skripsi ini. Semoga skripsi ini dapat melengkapi studi kajian Ilmu Komputer selanjutnya, khususnya dalam bidang *web security*. Terakhir, semoga skripsi ini bermanfaat bagi peneliti maupun orang lain di masa depan.

وَسَّلَامُ عَلَيْكُمْ وَرَحْمَةُ اللهِ وَبَرَكَاتُهُ

DAFTAR ISI

PERNYATAAN v
MOTTO vi
PERSEMBAHAN vii
KATA PENGANTAR viii
DAFTAR TABLE xii
DAFTAR GAMBAR ii
INTISARI iii
ABSTRACT iv
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 3
1.3 Batasan Masalah 4
1.4 Maksud dan Tujuan Penelitian 4
1.5 Manfaat Penelitian 4
1.6 Metode Penelitian 5
1.6.1 Metode Pengumpulan Data 5
1.6.2 Metode Analisis 5
1.6.3 Evaluasi Sistem 5
1.7 Sistematika Penulisan 5
BAB 1 : PENDAHULUAN 6
BAB II : LANDASAN TEORI 6
BAB III : ANALISIS DAN PERANCANGAN SISTEM 6
BAB IV : IMPLEMENTASI DAN PEMBAHASAN 6
BAB V : PENUTUP 6
BAB II LANDASAN TEORI 8
2.1 Kajian Pustaka 8
2.2 Dasar Teori 10
2.2.1 Api Endpoint Sistem 10
2.3 Kriptografi 11
2.3.1 Komponen- Komponen Kriptografi (istilah) 12
2.3.2 Tujuan Kriptografi 13
2.3.3 Algoritma kriptografi 14

2.4 Teknik Dasar Kriptografi 14
2.4.1 Kriptografi Klasik 14
2.4.2 Kriptografi Modern 17
2.5 Algoritma *Rijndael* 18
2.6 JSON 25
2.7 BASE64 28
2.7.1 Algoritma *Base* 64 encoding 29
2.7.2 Algoritma *Base 64 decoding* 30
2.8 SQL Injection 31
2.9 Man In The Middle (SNIFFING) 32
2.10 Penelitian Terdahulu 34
Penelitian terdahulu bertujuan untuk mendapatkan bahan perbandingan dan acuan 34
BAB III METODE PENELITIAN 40
3.1 Alur Penelitian 40
3.1.1 Menentukan topik dari penelitian 41
3.1.2 Melakukan studi literatur dan penetapan landasan teori 41
3.1.3 Pengumpulan dan Analisis Data 41
3.1.4 Mendefiniskan Permasalahan 41
3.1.5 Perancangan Sistem dan Penerapan Sistem 41
3.1.6 Pengujian Sistem 42
3.2 Analisis 45
3.2.1 Analisis Kebutuhan 45
3.2.2 Metode Analisis 47
BAB IV IMPLEMENTASI DAN PEMBAHASAN 54
4.1 Implementasi 54
4.1.1 Implementasi Design Interface 54
4.2 Pembahasan 55
4.2.1 Halaman API 55
4.3 Pengujian Sistem 58
4.3.1 Pengujian Serangan SQL Injection pada web tanpa algoritma SHA-256. 59
4.3.2 Pengujian serangan SQL Injection pada web dengan algoritma SHA-256 63
BAB V KESIMPULAN DAN SARAN 65
5.1 Kesimpulan 65
5.2 Saran 65

Daftar Pustaka 67

DAFTAR TABLE

Tabel 2. 1 Contoh Plaintext dan Chipertext 16
Tabel 2. 2 Konversi Binary, Decimal, Hexa 17
Tabel 2. 3 Contoh Kombinasi 2 bit atau XOR 18
Tabel 2. 4 Perbandingan jumlah proses pada algoritma Rijndael 19
Table 2. 5 Informasi Yang Dapat Diambil Dari Serangan Sniffing. 34
Tabel 2. 6 Penelitian Terdahulu……30
Tabel 2. 7 Penelitian Sekarang 31
Table 2.8 PERBEDAAN DAN KESAMAAN……32

DAFTAR GAMBAR

Gambar 2. 1 Proses Enkripsi dan Dekripsi Algoritma Rijndael 20
Gambar 2. 2 Proses yang dilalui pada saat AddRoundKey 22
Gambar 2. 3 Proses yang dilalui pada saat Subbytes 23
Gambar 2. 4 Proses yang dilalui pada saat shiftRow 23
Gambar 2. 5 Matrix Galois Field 24
Gambar 2. 6 Proses yang dilalui pada saat MixColumns 25
Gambar 2. 7 Algoritma Encoding Base 64 29
Gambar 2. 8 Algoritma Decoding Base 64 31
Gambar 3. 1 Flowchart Alur Penelitian 40
Gambar 3. 2 Flowchart Pengujian Web Dummy 43
Gambar 3. 3 Flowchart Web SHA-256 44
Gambar 3. 4 Flow Chart Client Server 46
Gambar 3. 5 Proses Pendekatan waterfall 48
Gambar 3. 6 Proses Hashing id berita dengan algoritma SHA-256 51
Gambar 3. 7 Perancangan antar muka halaman berita 53
Gambar 4. 1 data asli 55
Gambar 4. 2 REST-API Saat Data Tidak Ditemukan 55
Gambar 4. 3 Gambar Kode Halaman Berita 56
Gambar 4. 4 Gambar Koneksi Kode Dengan Salt 56
Gambar 4. 5 Gambar Kode Untuk Mendapatkan Log User 57
Gambar 4. 6 Karakter Regular Expression 58
Gambar 4. 7 Testing SQL Injection Union Select 59
Gambar 4. 8 Error Saat Url Disisipi Tanda Kutip 59
Gambar 4. 9 Hasil Awal Dari Union Select Query 61
Gambar 4. 10 Hasil Union Select 61
Gambar 4. 11 Dios Yang Harus Di Isi 62
Gambar 4. 12 Gambar Setelah Dios Di Isi 62
Gambar 4. 13 Data Yang Di Panggil 63
Gambar 4. 14 Ip Yang Ingin Masuk 64

INTISARI

Dewasa ini penggunaan REST-API sangat sering digunakan ketika melakukan pengembangan aplikasi.*Application Programming Interface* adalah salah satu cara untuk berkomunikasi antara *client-server* yang paling banyak digunakan saat ini baik pada aplikasi web, mobile, ataupun juga desktop , sedangkan REST (*Representational State Transfer*) merupakan salah satu *style* dari pengembangan *API* yang diakses menggunakan salah satu protocol TCP/IP yaitu HTTP/HTTPS untuk berkomunikasi dengan bentuk format data berupa JSON (*Javascript Object Notation)*, JSON adalah suatu format ringkas dalam melalukan pertukaran data berbasis text yang dapat dimengerti dan dibaca manusia serta digunakan dalam mempresentasikan struktur data yang disebut object.

Penelitian ini menggunakan Algoritma Rijndael untuk menjaga keamanan saat pemanggilan *API* yaitu pada saat request data hanya diperbolehkan dilakukan oleh pengguna yang sah dan juga mengamankan response data agar tidak terjadinya perubahan.

Penggunaan algoritma kriptografi pada penelitian ini dimaksudkan agar komunikasi data tidak dapat disadap oleh pihak yang tidak sah. Hasil dari penilitian ini aplikasi *REST-API* tidak dapat disadap dan berhasil menghindari serangan tidak dapat disadap dan berhasil menghindari serangan cryptanalysis.

Kata Kunci : *REST-API, JSON , AES , RIJNDAEL*

ABSTRACT

Nowadays, the use of REST-API is very often used when developing applications. Application Programming Interface is one of the most widely used ways to communicate between client-servers in web, mobile or desktop applications, while REST (Representational State Transfer)) is one of the styles of API development that is accessed using one of the TCP / IP protocols, namely HTTP / HTTPS to communicate in the form of a data format in the form of JSON (Javascript Object Notation), JSON is a short format for exchanging text-based data that is understandable and human read and used in presenting data structures called objects.

This study uses the Rijndael Algorithm to maintain security when calling the API, namely when data requests are only allowed to be made by authorized users and also secure the data response so that changes do not occur.

The use of cryptographic algorithms in this study is intended so that unauthorized parties cannot intercept data communications. The results of this study that the REST-API application cannot be intercepted and managed to avoid attacks cannot be tapped and managed to avoid cryptanalysis attacks.

Keyword : REST-API, JSON , AES , RIJNDAEL