IMPLEMENTASI GALOIS/COUNTER MODE (GCM) UNTUK KEAMANAN DATA PADA SISTEM PENGADAAN BERBASIS WEB DENGAN METODE RIJNDAEL

SKRIPSI

Steven Geraldi
00000043822

PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS MULTIMEDIA NUSANTARA
TANGERANG
2024

IMPLEMENTASI GALOIS/COUNTER MODE (GCM) UNTUK KEAMANAN DATA PADA SISTEM PENGADAAN BERBASIS WEB DENGAN METODE RIJNDAEL

SKRIPSI

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

Steven Geraldi
00000043822

PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS MULTIMEDIA NUSANTARA
TANGERANG
2024

HALAMAN PERNYATAAN TIDAK PLAGIAT

Dengan ini saya,

Nama	:	Steven Geraldi
Nomor Induk Mahasiswa	:	00000043822
Program Studi	:	Informatika

Menyatakan dengan sesungguhnya bahwa Skripsi saya yang berjudul:
Implementasi Galois/Counter Mode (GCM) untuk Keamanan Data pada Sistem Pengadaan Berbasis Web dengan Metode Rijndael

merupakan hasil karya saya sendiri, bukan merupakan hasil plagiat, dan tidak pula dituliskan oleh orang lain; Semua sumber, baik yang dikutip maupun dirujuk, telah saya cantumkan dan nyatakan dengan benar pada bagian Daftar Pustaka.

Jika di kemudian hari terbukti ditemukan kecurangan/penyimpangan, baik dalam pelaksanaan skripsi maupun dalam penulisan laporan karya ilmiah, saya bersedia menerima konsekuensi untuk dinyatakan TIDAK LULUS. Saya juga bersedia menanggung segala konsekuensi hukum yang berkaitan dengan tindak plagiarisme ini sebagai kesalahan saya pribadi dan bukan tanggung jawab Universitas Multimedia Nusantara.

Tangerang, 15 Mei 2024

(Steven Geraldi)

HALAMAN PENGESAHAN

Skripsi dengan judul

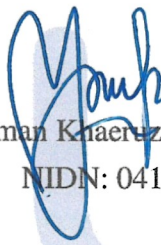
IMPLEMENTASI GALOIS/COUNTER MODE (GCM) UNTUK KEAMANAN DATA PADA SISTEM PENGADAAN BERBASIS WEB DENGAN METODE RIJNDAEL

oleh

Nama	:	Steven Geraldi
NIM	:	00000043822
Program Studi	:	Informatika
Fakultas	:	Fakultas Teknik dan Informatika

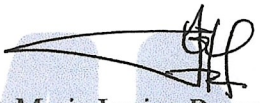
Telah diujikan pada hari Kamis, 30 Mei 2024
Pukul 13.00 s/s 15.00 dan dinyatakan
LULUS
Dengan susunan penguji sebagai berikut

Ketua Sidang



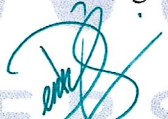
(Yaman Khaeruzzaman, M.Sc.)
NIDN: 0413057104

Penguji



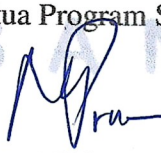
(Dr. Maria Irmina Prasetiyowati, S.Kom., M.T.)
NIDN: 0725057201

Pembimbing



(Dennis Gunawan, S.Kom., M.Sc.)
NIDN: 0320059001

Pjs Ketua Program Studi Informatika,



(Dr. Eng. Niki Prastomo, S.T., M.Sc.)
NIDN: 0419128203

LEMBAR PERSETUJUAN PUBLIKASI
KARYA ILMIAH MAHASISWA

Yang bertanda tangan dibawah ini:

Nama	: Steven Geraldi
Nomor Induk Mahasiswa	: **00000043822**
Program Studi	: Informatika
Jenjang	: S1
Judul Karya Ilmiah	:

Implementasi Galois/Counter Mode (GCM) untuk Keamanan Data pada Sistem Pengadaan Berbasis Web dengan Metode Rijndael

Menyatakan dengan sesungguhnya bahwa saya bersedia:

☑ Memberikan izin sepenuhnya kepada Universitas Multimedia Nusantara untuk mempublikasikan hasil karya ilmiah saya di repositori Knowledge Center, sehingga dapat diakses oleh Civitas Akademika/Publik. Saya menyatakan bahwa karya ilmiah yang saya buat tidak mengandung data yang bersifat konfidensial dan saya juga tidak akan mencabut kembali izin yang telah saya berikan dengan alasan apapun.

Saya tidak bersedia, dikarenakan:

☐ Dalam proses pengajuan untuk diterbitkan ke jurnal/konferensi nasional/internasional (dibuktikan dengan *letter of acceptance*) *.

Tangerang, 15 Mei 2024

(Steven Geraldi)

* Jika tidak bisa membuktikan LoA jurnal/HKI selama 6 bulan kedepan, saya bersedia mengizinkan penuh karya ilmiah saya untuk diunggah ke KC UMN dan menjadi hak institusi UMN.

Halaman Persembahan / Motto

"*Don't let fear hold you back. Fear is just a thought, and thoughts can be controlled. Embrace the unknown, and you'll find your true potential.*"

-Andrew Tate

KATA PENGANTAR

Puji Syukur atas berkat dan rahmat kepada Tuhan Yang Maha Esa, atas selesainya penulisan laporan Skripsi ini dengan judul: Implementasi Galois/Counter Mode (GCM) untuk Keamanan Data pada Sistem Pengadaan Berbasis Web dengan Metode Rijndael 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. Bapak Dr. Eng. Niki Prastomo, S.T., M.Sc., selaku Dekan Fakultas Teknik dan Informatika Universitas Multimedia Nusantara.
3. Bapak Dr. Eng. Niki Prastomo, S.T., M.Sc., selaku Pjs Ketua Program Studi Informatika Universitas Multimedia Nusantara.
4. Bapak Dennis Gunawan, S.Kom., M.Sc., sebagai Pembimbing pertama yang telah banyak meluangkan waktu untuk memberikan bimbingan, arahan dan motivasi atas terselesainya skripsi ini.
5. Keluarga dan pacar saya yang telah memberikan bantuan dukungan moral, sehingga penulis dapat menyelesaikan skripsi ini.

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

Tangerang, 15 Mei 2024

Steven Geraldi

IMPLEMENTASI GALOIS/COUNTER MODE (GCM) UNTUK KEAMANAN DATA PADA SISTEM PENGADAAN BERBASIS WEB DENGAN METODE RIJNDAEL

Steven Geraldi

ABSTRAK

Keamanan informasi menjadi suatu aspek kritis dalam pengelolaan data pada era digital ini, terutama ketika ada sistem yang melibatkan basis data untuk menyimpan informasi rahasia dan bernilai tinggi seperti yang ada pada sebuah sistem pengadaan. Sistem pengadaan menyimpan data *supplier* yang tidak boleh jatuh ke orang yang tidak bertanggung jawab karena setiap perusahaan akan memilih *supplier* yang terbaik untuk memastikan keunggulan produk atau jasanya. Untuk mencegah terjadinya kebocoran data, perusahaan dapat mengimplementasikan *Galois/Counter Mode* pada sistem pengadaan berbasis *web* dengan metode *Rijndael*. Hasil penelitian dibagi menjadi dua, yaitu penilaian oleh pakar dan *benchmark* durasi enkripsi dan dekripsi AES-GCM. Pakar menilai keamanan sistem dengan melakukan *vulnerability assessment*. *Vulnerability assessment* dilakukan dengan menggunakan tiga *automated tools*, yaitu PentestTools, HostedScan, dan Acunetix. Hasil dari ketiga *tools* tersebut menunjukkan bahwa *threat level* sistem pengadaan ini berada di level *medium* dengan beberapa kerentanan yang ditemukan juga. Akan tetapi, seluruh kerentanan tersebut tidak ada yang berhubungan dengan *cryptography*. *Benchmark* durasi enkripsi untuk *plaintext* dengan ukuran 12-72 *byte* pada *environment production* adalah 3631-4323 *nanosecond* pada *environment production*. *Benchmark* durasi dekripsi pada *plaintext* dengan panjang 12-72 *byte* yang sudah dienkripsi adalah 1028-1243 *nanosecond*.

Kata kunci: AES, GCM, AES-GCM, kriptografi, *Supplier Master Data*

Implementation of Galois/Counter Mode (GCM) for Data Security in Web-Based Procurement System using Rijndael Method

Steven Geraldi

ABSTRACT (English)

In today's digital age, information security has become a critical aspect of data management, particularly in systems that involve databases for storing sensitive and valuable information like those found in procurement systems. Procurement systems store supplier data that must be protected from unauthorized access, as companies carefully select suppliers to ensure the superiority of their products or services. To prevent data breaches, companies can implement Galois/Counter Mode (GCM) on web-based procurement systems using the Rijndael method. This research finding was conducted in expert evaluation and benchmarking of AES-GCM encryption and decryption durations. The security of the procurement system was assessed by experts using a vulnerability assessment. Three automated methods, PentestTools, HostedScan, and Acunetix, assisted the assessment. The results from these tools indicated that the system's threat level is medium, with some vulnerabilities identified. However, none of these vulnerabilities were related to cryptography. Encryption and decryption speed benchmarks were conducted for plaintexts ranging from 12 to 72 bytes in a production environment. The results showed that encryption durations ranged from 3631 to 4323 nanoseconds, while decryption durations ranged from 1028 to 1243 nanoseconds.

Keywords: *AES, GCM, AES-GCM, Cryptography, Supplier Master Data*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR KODE

DAFTAR LAMPIRAN