

**PENERAPAN KRIPTOGRAFI AES-256-GCM PADA APLIKASI  
BERBASIS RESTAURANT MANAGEMENT SYSTEM (RMS)  
UNTUK KEAMANAN DATA TRANSAKSI  
(STUDI KASUS : KEDAI TALOK FRIED CHICKEN BACIRO)**

**TUGAS AKHIR**



**Difa Amzar Hafiy**

**NIM. 20106050002**

**STATE ISLAMIC UNIVERSITY  
SUNAN KALIJAGA  
YOGYAKARTA  
PROGRAM STUDI INFORMATIKA  
FAKULTAS SAINS DAN TEKNOLOGI  
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA  
YOGYAKARTA**

**2024**



**KEMENTERIAN AGAMA  
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA  
FAKULTAS SAINS DAN TEKNOLOGI**

Jl. Marsda Adisucipto Telp. (0274) 540971 Fax. (0274) 519739 Yogyakarta 55281

**PENGESAHAN TUGAS AKHIR**

Nomor : B-1205/Un.02/DST/PP.00.9/07/2024

Tugas Akhir dengan judul : Penerapan Kriptografi AES-256-GCM Pada Aplikasi Berbasis Restaurant Management System (RMS) Untuk Meningkatkan Keamanan Data Transaksi (Studi Kasus : Kedai Talok Fried Chicken Baciro)

yang dipersiapkan dan disusun oleh:

Nama : DIFA AMZAR HAFIY  
Nomor Induk Mahasiswa : 20106050002  
Telah diujikan pada : Jumat, 19 Juli 2024  
Nilai ujian Tugas Akhir : A-

dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta

**TIM UJIAN TUGAS AKHIR**



Ketua Sidang

Dr. Ir. Bambang Sugiantoro, M.T., IPU., ASEAN Eng.  
SIGNED

Valid ID: 66a31cf464af4



Penguji I

Ir. Muhammad Taufiq Nuruzzaman, S.T.  
M.Eng., Ph.D.  
SIGNED

Valid ID: 66a31b89c70f9



Penguji II

Mandahadi Kusuma, M.Eng.  
SIGNED

Valid ID: 66a1b4c28a399



Yogyakarta, 19 Juli 2024

UIN Sunan Kalijaga  
Dekan Fakultas Sains dan Teknologi

Prof. Dr. Dra. Hj. Khurul Wardati, M.Si.  
SIGNED

Valid ID: 66a336738f820

## LEMBAR PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : Difa Amzar Hafiy  
NIM : 20106050002  
Dosen Pembimbing : Dr. Ir. Bambang Sugiantoro, M.T., IPU., ASEAN Eng.  
Program Studi : Informatika  
Fakultas : Sains dan Teknologi

Menyatakan bahwa tugas akhir saya yang berjudul "*Penerapan Kriptografi AES-256-GCM Pada Aplikasi Berbasis Restaurant Management System (RMS) Untuk Meningkatkan Keamanan Data Transaksi (Studi Kasus : Kedai Talok Fried Chicken Baciro)*" merupakan hasil penelitian saya sendiri, tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu perguruan tinggi, dan sepanjang sepengetahuan saya, tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka. Selain itu juga tugas akhir ini diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Program Studi Informatika Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga.

STATE ISLAMIC UNIVERSITY  
SUNAN KALIJAGA  
YOGYAKARTA

Yogyakarta, 15 Juli 2024

Yang Menyatakan,



**Difa Amzar Hafiy**  
**NIM. 20106050002**



## LEMBAR PERSETUJUAN

Hal : Persetujuan Tugas Akhir

Lamp : -

Kepada

Yth. Dekan Fakultas Sains dan Teknologi  
UIN Sunan Kalijaga Yogyakarta

Assalamua'laikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta melakukan perbaikan seperlunya, maka saya selaku pembimbing berpendapat bahwa tugas akhir Saudara :

Nama : Difa Amzar Hafiy

NIM : 20106050002

Judul Tugas Akhir : Penerapan Kriptografi AES-256-GCM Pada Aplikasi Berbasis Restaurant Management System (RMS) Untuk Meningkatkan Keamanan Data Transaksi (Studi Kasus : Kedai Talok Fried Chicken Baciro)

Sudah dapat diajukan kepada Program Studi Informatika UIN Sunan Kalijaga dalam rangka memperoleh gelar Sarjana Informatika.

Wassalamua'laikum wr. wb.

Yogyakarta, 15 Juli 2024

Pembimbing,

**Dr. Ir. Bambang Sugiantoro, M.T., IPU., ASEAN Eng.**

**NIP: 19751024 200912 1 002**

## LEMBAR PEDOMAN PENGGUNAAN TUGAS AKHIR

*Tugas Akhir ini tidak dipublikasikan, tetapi tersedia di perpustakaan dalam lingkungan UIN Sunan Kalijaga Yogyakarta, diperkenankan dipakai sebagai referensi kepustakaan, tetapi pengutipan harus seizin penyusun, dan harus menyebutkan sumbernya sesuai dengan kebiasaan ilmiah. Dokumen Tugas Akhir ini merupakan hak milik UIN Sunan Kalijaga Yogyakarta.*



## HALAMAN PERSEMBAHAN

Atas karunia Allah SWT penulis persembahkan Tugas Akhir ini kepada :

Dadan Ramdani S.Pd.I

Selaku ayah tercinta

Atis Trisnawati

Selaku ibu tercinta

Fakhri Muhammad Fauzan dan Azkiya Sofura Husna

Selaku adik tersayang

Semua sahabat dan teman seperjuangan Informatika angkatan 2020

Yang selalu memberikan dukungan tak terbatas untuk penulis

Serta

Almamater tercinta

**Program Studi Informatika**

**Fakultas Sains dan Teknologi**

**Universitas Islam Negeri Sunan Kalijaga Yogyakarta**

STATE ISLAMIC UNIVERSITY  
SUNAN KALIJAGA  
YOGYAKARTA

## ABSTRAK

Kedai Talok Fried Chicken Baciro saat ini menjual produknya melalui aplikasi pihak ketiga seperti Shopee dan GoFood, yang rawan terhadap ancaman manipulasi data transaksi dan kedai ini juga belum memiliki aplikasi pemesanan sendiri. Untuk meningkatkan keamanan data transaksi, maka dibuatlah aplikasi dengan model Restaurant Management System (RMS) yang aksesnya berlaku untuk admin dan pegawai (pelayan, kasir, dan dapur). Aplikasi ini dilengkapi dengan fitur keamanan kriptografi.

Implementasi RMS ini bertujuan untuk mempermudah pengelolaan pesanan, stok barang, dan mengamankan data transaksi, serta mengurangi ketergantungan pada platform pihak ketiga. Metode kriptografi yang digunakan adalah AES-256-GCM dengan workshop design RAD, PHP dan Bootstrap digunakan sebagai tools pendukung untuk membuat serta mengembangkan aplikasi ini.

Hasil penelitian menunjukkan data transaksi seperti identitas pelanggan dan struk pembayaran dapat di enkripsi oleh user pelayan dan kasir serta tersimpan otomatis di database, dan dapat di dekripsi secara otomatis oleh user admin. Selain implementasi kriptografi, terdapat juga pengujian dan evaluasi pada aplikasi RMS yang telah dibuat.

**Kata kunci:** *Kriptografi, AES-256-GCM, Restaurant Management System (RMS), Keamanan Data Transaksi, Kedai Talok Fried Chicken Baciro*



## ABSTRACT

*The Talok Fried Chicken Baciro shop currently sells its products through third party applications such as Shopee and GoFood, which are vulnerable to threats of manipulation of transaction data and this shop also does not have its own ordering application. To increase the security of transaction data, an application was created with a Restaurant Management System (RMS) model whose access applies to admin and employees (waiters, cashiers and kitchen). This application is equipped with cryptographic security features.*

*This RMS implementation aims to make it easier to manage orders, stock of goods, and secure transaction data, as well as reducing dependence on third-party platforms. The cryptographic method used is AES-256-GCM with RAD, PHP and Bootstrap design workshops used as supporting tools to create and develop this application.*

*The research results show that transaction data such as customer identity and payment receipts can be encrypted by waiter and cashier users and stored automatically in the database, and can be decrypted automatically by admin users. Apart from implementing cryptography, there is also testing and evaluation of the RMS applications that have been created.*

**Keywords:** *Cryptography, AES-256-GCM, Restaurant Management System (RMS), Transaction Data Security, Talok Fried Chicken Baciro Shop*





## KATA PENGANTAR

*Assalamu'alaikum Wr. Wb.*

Puja dan puji syukur marilah kita bersama-sama panjatkan kepada dzat Alloh SWT sang Khalik pencipta sekalian alam, yang telah memberikan kesehatan kepada kita semua baik kesehatan lahir maupun batin. Sholawat beserta salam marilah kita sanjungkan kepada Nabi akhir zaman yakni Nabi Muhammad SAW.

Dalam rancang bangun pengembangan sistem tugas akhir ini, saya selaku penulis akan memaparkan judul tentang *“Penerapan Kriptografi AES-256-GCM Pada Aplikasi Berbasis Restaurant Management System (RMS) Untuk Meningkatkan Keamanan Data Transaksi (Studi Kasus : Kedai Talok Fried Chicken Baciro)”*.

Rasa syukur yang mendalam dan ucapan terima kasih saya persembahkan kepada :

1. Allah SWT yang telah memberikan kelancaran kepada penulis untuk menyelesaikan tugas akhir ini.
2. Kedua Orang Tua saya yang telah memotivasi dalam hal apapun, memberikan perhatian dan kasing sayang yang tiada tara, serta senantiasa mendoakan untuk tercapainya keberhasilan penelitian tugas akhir ini.
3. Prof. Dr. Phil. Al Makin, S.Ag. MA. Selaku Rektor UIN Sunan Kalijaga Yogyakarta.
4. Prof. Dr. Dra Hj. Khurul Wardati, M.Si. Selaku Dekan Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta.
5. Ir. Maria Ulfah Siregar, S.Kom., MIT., Ph.D. selaku Ketua Program Studi Teknik Informatika.
6. Eko Hadi Gunawan, M.Eng. selaku Dosen Pembimbing Akademik.
7. Dr. Ir. Bambang Sugiantoro, M.T., IPU., ASEAN Eng. selaku Dosen Pembimbing Skripsi.
8. Pak Teguh, Selaku Owner atau Pemilik Kedai Talok Fried Chicken Baciro.
9. Amin Sahri S.Sos, selaku Owner atau Pemilik P.T. Rindu Buku x Rindu Express Yogyakarta di tempat kerja part time saya, yang sudah membantu mengarahkan dan menjadi koneksi saya supaya bisa melakukan penelitian di Kedai Talok Fried Chicken Baciro.

10. Pembuat sumber informasi dan referensi dalam tugas akhir ini.
11. Pihak-pihak yang telah membantu dalam proses pembuatan tugas akhir ini yang tidak dapat disebutkan penulis satu persatu.

Semoga dengan penelitian tugas akhir yang saya paparkan ini bisa memberikan manfaat, menambah pengetahuan dan wawasan bagi khalayak umum.

*Wassalamu'alaikum Wr. Wb.*

Yogyakarta, 7 Juli 2024

Penyusun,



**Difa Amzar Hafiy**  
**NIM. 20106050002**



STATE ISLAMIC UNIVERSITY  
SUNAN KALIJAGA  
YOGYAKARTA

## DAFTAR ISI

<b>HALAMAN JUDUL</b> .....	i
<b>LEMBAR PENGESAHAN</b> .....	ii
<b>LEMBAR PERNYATAAN</b> .....	iii
<b>LEMBAR PERSETUJUAN</b> .....	iv
<b>LEMBAR PEDOMAN PENGGUNAAN TUGAS AKHIR</b> .....	v
<b>HALAMAN PERSEMBAHAN</b> .....	vi
<b>ABSTRAK</b> .....	vii
<b>ABSTRACT</b> .....	viii
<b>KATA PENGANTAR</b> .....	ix
<b>DAFTAR ISI</b> .....	xi
<b>DAFTAR TABEL</b> .....	xiv
<b>DAFTAR GAMBAR</b> .....	xv
<b>DAFTAR LAMPIRAN</b> .....	xvii
<b>BAB I PENDAHULUAN</b> .....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah .....	3
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian.....	4
1.5 Manfaat Penelitian.....	4
<b>BAB II KAJIAN PUSTAKA</b> .....	5
2.1 Kajian Pustaka.....	5
2.1.1 Teori Pengembangan Sistem .....	12
<b>BAB III METODE PENGEMBANGAN SISTEM</b> .....	21
3.1 Requirements Planning Studi Kasus Penelitian.....	22
3.1.1 Objek Penelitian .....	22
3.1.2 Alat dan Bahan .....	22
3.2 Pengembangan Sistem RMS .....	23
3.3 Sistem Kriptografi AES-256-GCM.....	23
3.4 Implementasi Kriptografi AES-256-GCM Pada Aplikasi RMS .....	23
3.5 Pengujian dan Evaluasi Keamanan Pada Aplikasi RMS .....	24
<b>BAB IV PERANCANGAN DAN EVALUASI SISTEM</b> .....	25

4.1 Requirements Planning Aplikasi RMS .....	25
4.2 Workshop Design RAD Aplikasi RMS .....	26
4.2.1 Use Case Diagram RMS .....	27
4.2.2 Activity Diagram (Flowchart) RMS .....	29
4.2.3 Class Diagram RMS .....	30
4.2.4 Entity Relationship Diagram (ERD) RMS .....	31
4.2.5 Sequence Diagram Login RMS.....	32
4.2.6 Sequence Diagram Membuat Order Pesanan RMS .....	33
4.2.7 Sequence Diagram Kelola Menu, User, dan Laporan RMS.....	34
4.2.8 Sequence Diagram Kelola Dapur RMS .....	35
4.3 Implementasi Workshop Desain RAD Pada Aplikasi RMS .....	35
4.3.1 Tampilan Login Aplikasi RMS Kedai Talok .....	35
4.3.2 Tampilan Dashboard Semua User Role Aplikasi RMS Kedai Talok .....	36
4.3.3 Tampilan Daftar Menu Aplikasi RMS Kedai Talok .....	38
4.3.4 Tampilan Kategori Menu Aplikasi RMS Kedai Talok .....	39
4.3.5 Tampilan Menu User Aplikasi RMS Kedai Talok.....	39
4.3.6 Tampilan Menu Order Aplikasi RMS Kedai Talok.....	40
4.3.7 Tampilan Menu Order Item Aplikasi RMS Kedai Talok .....	40
4.3.8 Tampilan Menu Pembayaran Aplikasi RMS Kedai Talok .....	41
4.3.9 Tampilan Struk Pembayaran Aplikasi RMS Kedai Talok.....	42
4.3.10 Tampilan Menu Dapur Aplikasi RMS Kedai Talok .....	42
4.3.11 Tampilan Menu Report Aplikasi RMS Kedai Talok .....	43
4.3.12 Tampilan Menu View Item Aplikasi RMS Kedai Talok .....	44
4.4 Skema dan Workshop Desain Kriptografi Pada Aplikasi RMS Kedai Talok .....	44
4.4.1 Skema Kriptografi AES-256-GCM Pada Aplikasi RMS Kedai Talok.....	44
4.4.2 Workshop Desain Kriptografi Pada Aplikasi RMS Kedai Talok .....	46
4.5 Implementasi Kriptografi AES-256-GCM Pada Aplikasi RMS Kedai Talok.....	49
4.5.1 Proses Enkripsi AES-256-GCM Pada Aplikasi RMS Kedai Talok.....	49
4.5.2 Proses Dekripsi AES-256-GCM Pada Aplikasi RMS Kedai Talok .....	53
4.6 Pengujian dan Evaluasi Keamanan Pada Aplikasi RMS Kedai Talok Dengan.....	55
OWASP ZAP .....	
4.6.1 Pengujian dan Evaluasi Keamanan Pada Aplikasi RMS Kedai Talok .....	56
Dengan Fungsi Kriptografi.....	

4.6.2 Pengujian dan Evaluasi Keamanan Pada Aplikasi RMS Kedai Talok .....	62
Tanpa Fungsi Kriptografi .....	
<b>BAB V PENUTUP</b> .....	69
5.1 Kesimpulan .....	69
5.2 Saran .....	69
<b>DAFTAR PUSTAKA</b> .....	xviii
<b>LAMPIRAN</b> .....	xx
<b>CONTACT PERSON</b> .....	xxiii



## DAFTAR TABEL

<i>Tabel 1. Ringkasan Hasil Kajian Pustaka .....</i>	<i>7</i>
<i>Tabel 2. Perbandingan Model Kriptografi .....</i>	<i>11</i>
<i>Tabel 3. Jumlah Putaran Algoritma AES Versi 1 .....</i>	<i>15</i>
<i>Tabel 4. Jumlah Putaran Algoritma AES Versi 2 .....</i>	<i>16</i>
<i>Tabel 5. Alat (Hardware).....</i>	<i>22</i>
<i>Tabel 6. Bahan (Software) .....</i>	<i>22</i>
<i>Tabel 7. Requirements Planning Aplikasi RMS.....</i>	<i>26</i>



## DAFTAR GAMBAR

<i>Gambar 1. Metode Rapid Application Development (RAD).....</i>	<i>13</i>
<i>Gambar 2. Skema Kriptografi.....</i>	<i>15</i>
<i>Gambar 3. Proses Enkripsi Algoritma AES-256.....</i>	<i>17</i>
<i>Gambar 4. Proses Dekripsi Algoritma AES-256.....</i>	<i>18</i>
<i>Gambar 5. Metode Pengembangan Sistem.....</i>	<i>21</i>
<i>Gambar 6. Use Case Diagram (RMS) Kedai Talok.....</i>	<i>28</i>
<i>Gambar 7. Activity Diagram (RMS) Kedai Talok.....</i>	<i>29</i>
<i>Gambar 8. Class Diagram (RMS) Kedai Talok.....</i>	<i>31</i>
<i>Gambar 9. ERD (RMS) Kedai Talok.....</i>	<i>32</i>
<i>Gambar 10. Sequence Diagram Login (RMS) Kedai Talok.....</i>	<i>33</i>
<i>Gambar 11. Sequence Diagram Order Pesanan (RMS) Kedai Talok.....</i>	<i>34</i>
<i>Gambar 12. Sequence Diagram Kelola Menu, User, &amp; Laporan (RMS) Kedai Talok.....</i>	<i>34</i>
<i>Gambar 13. Sequence Diagram Kelola Dapur (RMS) Kedai Talok.....</i>	<i>35</i>
<i>Gambar 14. Tampilan Login Aplikasi RMS Kedai Talok.....</i>	<i>36</i>
<i>Gambar 15. Tampilan Dashboard User Admin.....</i>	<i>36</i>
<i>Gambar 16. Tampilan Dashboard User Pelayan.....</i>	<i>37</i>
<i>Gambar 17. Tampilan Dashboard User Kasir.....</i>	<i>37</i>
<i>Gambar 18. Tampilan Dashboard User Dapur.....</i>	<i>38</i>
<i>Gambar 19. Tampilan Daftar Menu Aplikasi RMS Kedai Talok.....</i>	<i>38</i>
<i>Gambar 20. Tampilan Kategori Menu Aplikasi RMS Kedai Talok.....</i>	<i>39</i>
<i>Gambar 21. Tampilan Menu User Aplikasi RMS Kedai Talok.....</i>	<i>40</i>
<i>Gambar 22. Tampilan Menu Order Aplikasi RMS Kedai Talok.....</i>	<i>40</i>
<i>Gambar 23. Tampilan Menu Order Item Aplikasi RMS Kedai Talok.....</i>	<i>41</i>
<i>Gambar 24. Tampilan Menu Pembayaran Aplikasi RMS Kedai Talok.....</i>	<i>42</i>
<i>Gambar 25. Tampilan Struk Pembayaran Aplikasi RMS Kedai Talok.....</i>	<i>42</i>
<i>Gambar 26. Tampilan Menu Dapur Aplikasi RMS Kedai Talok.....</i>	<i>43</i>
<i>Gambar 27. Tampilan Menu Report Aplikasi RMS Kedai Talok.....</i>	<i>43</i>
<i>Gambar 28. Tampilan Menu View Item Aplikasi RMS Kedai Talok.....</i>	<i>44</i>
<i>Gambar 29. Skema Kriptografi Pada Aplikasi RMS Kedai Talok.....</i>	<i>45</i>
<i>Gambar 30. Class Diagram Kriptografi RMS.....</i>	<i>47</i>
<i>Gambar 31. Sequence diagram membuat order pesanan (Kriptografi RMS).....</i>	<i>48</i>

<i>Gambar 32. Sequence diagram kelola laporan/report (Kriptografi RMS).....</i>	<i>49</i>
<i>Gambar 33. Order Pesanan Oleh User Pelayan di Menu Order.....</i>	<i>50</i>
<i>Gambar 34. Tampilan data pelanggan terenkripsi di menu order oleh pelayan .....</i>	<i>50</i>
<i>Gambar 35. Data pelanggan terenkripsi di menu order item oleh pelayan .....</i>	<i>51</i>
<i>Gambar 36. Data transaksi terenkripsi di struk pembayaran oleh pelayan.....</i>	<i>51</i>
<i>Gambar 37. Order Pesanan Oleh User Kasir di Menu Order.....</i>	<i>52</i>
<i>Gambar 38. Tampilan data pelanggan terenkripsi di menu order oleh kasir .....</i>	<i>52</i>
<i>Gambar 39. Data pelanggan terenkripsi di menu order item oleh kasir.....</i>	<i>53</i>
<i>Gambar 40. Data transaksi terenkripsi di struk pembayaran oleh kasir.....</i>	<i>53</i>
<i>Gambar 41. Data pribadi pelanggan terdekripsi di menu report oleh admin.....</i>	<i>54</i>
<i>Gambar 42. Data pelanggan dari user role pelayan dan kasir masuk di menu report .....</i>	<i>54</i>
<i>Gambar 43. Rincian detail order pesanan user pelayan di menu view item .....</i>	<i>55</i>
<i>Gambar 44. Rincian detail order pesanan user kasir di menu view item.....</i>	<i>55</i>
<i>Gambar 45. Testing&amp;Evaluasi Aplikasi RMS Kedai Talok Kriptografi di OWASP ZAP ..</i>	<i>57</i>
<i>Gambar 46. Membuat konteks scan attack di OWASP ZAP .....</i>	<i>57</i>
<i>Gambar 47. Proses Otentikasi di OWASP ZAP .....</i>	<i>58</i>
<i>Gambar 48. Proses input user dan password di OWASP ZAP .....</i>	<i>58</i>
<i>Gambar 49. Tahap Memulai Scan Attack di OWASP ZAP .....</i>	<i>59</i>
<i>Gambar 50. Proses Memulai Scan Attack di OWASP ZAP .....</i>	<i>59</i>
<i>Gambar 51. Hasil Scan Attack Aplikasi RMS Kedai Talok Berbasis Kriptografi.....</i>	<i>60</i>
<i>Gambar 52. Hasil Scan Attack Aplikasi RMS Kedai Talok Tanpa Kriptografi .....</i>	<i>62</i>



## DAFTAR LAMPIRAN

Lampiran 1. Data Hasil Enkripsi Kriptografi AES-256-GCM Pada Aplikasi.....	xx
RMS Kedai Talok .....	
Lampiran 2. Data Hasil Dekripsi Kriptografi AES-256-GCM Pada Aplikasi.....	xxi
RMS Kedai Talok .....	
Lampiran 3. Data Hasil Pengujian Aplikasi RMS Dengan Fungsi Kriptografi.....	xxii
Lampiran 4. Data Hasil Pengujian Aplikasi RMS Tanpa Fungsi Kriptografi .....	xxii



# **BAB I**

## **PENDAHULUAN**

### **1.1 Latar Belakang**

Kedai Talok Fried Chicken Baciro merupakan salah satu usaha kuliner yang beroperasi di Jl. Tri Dharma, Gendeng Baciro, Kec. Gondokusuman, Kota Yogyakarta. Selama ini, Kedai Talok Fried Chicken menjual produk makanan dan minumannya melalui aplikasi pihak ketiga seperti Shopee dan GoFood. Meskipun penggunaan aplikasi pihak ketiga tersebut telah dijalankan untuk upaya menjangkau pelanggan yang lebih luas, namun untuk hasilnya masih jauh dari harapan. Hal ini disebabkan oleh berbagai faktor, termasuk adanya pembagian komisi dengan aplikasi pihak ketiga, kurangnya kontrol langsung terhadap proses pemesanan, dan keterbatasan dalam mengelola data pelanggan serta data transaksi. Oleh karena itu, dibuatlah sebuah aplikasi yang dapat mengelola operasional kedai secara lebih efisien, aman, dan terintegrasi. Pemilik kedai juga lebih menginginkan aplikasi yang dapat dikontrol penuh oleh admin dan beroperasi di lingkungan internal saja, kemudian untuk jangkauan pelanggan juga lebih banyak dari daerah yang dekat kedai saja atau masih dalam satu daerah, dan dari hasil analisis kebanyakan pelanggan lebih banyak yang datang langsung ke kedai daripada memesan online lewat Shopee ataupun GoFood. Maka dengan itu untuk mengoptimalkan pendapatan dan efisiensi operasional kedai dibuatlah aplikasi pemesanan makanan dengan model Restaurant Management System (RMS).

Restaurant Management System (RMS) adalah teknologi berbasis web untuk mengelola bisnis restoran menjadi lebih baik. RMS menyediakan wadah yang terintegrasi untuk mengelola bahan baku hingga menjadi makanan siap saji dan berfungsi sebagai pusat pengelolaan, sehingga pelayan dan chef atau bagian dapur dapat mengelola dan melakukan kegiatan operasional [1]. Aplikasi ini dirancang khusus untuk kebutuhan internal kedai, dengan akses yang terbatas hanya untuk pegawai, termasuk admin (owner), pelayan, kasir, dan bagian dapur. Sistem ini diharapkan dapat mempermudah pengelolaan pesanan, stok barang, dan transaksi keuangan, serta mengurangi ketergantungan pada platform pihak ketiga. Selain itu, RMS ini dilengkapi dengan fitur keamanan kriptografi menggunakan algoritma AES-256-GCM, yang berfungsi untuk melindungi kerahasiaan dan integritas data transaksi dari potensi ancaman keamanan seperti pencurian data atau manipulasi informasi, contohnya yaitu seperti kejahatan digital cybercrime.

Cybercrime merupakan ancaman keamanan yang dapat terjadi karena adanya celah atau kerentanan pada sistem, yang dapat dieksploitasi oleh kejahatan di dunia maya untuk mengeksploitasi sistem tersebut, dan menyebabkan hilangnya prinsip keamanan. Ada empat macam ancaman dalam cybercrime, yaitu penyadapan (interception), pemalsuan (fabrication), modifikasi, dan gangguan (interruption) [2]. Sebuah algoritma diperlukan untuk menyandikan data sensitif sehingga orang yang tidak memiliki hak akses tidak dapat mengetahui apa yang ada dalam data tersebut, contohnya dengan menggunakan metode kriptografi AES. Kriptografi merupakan teknik mengamankan dan menyandikan data atau informasi, atau bisa disebut juga seni melindungi data dengan menggunakan teknik matematika. Dan kriptografi itu sendiri adalah bagian dari cabang ilmu matematika yang disebut kriptologi (cryptologi) [3]. Tujuannya agar orang dari pihak ketiga tidak dapat memanipulasi data atau informasi tersebut. Salah satu algoritma kriptografi yang populer adalah Advanced Encryption Standard (AES). AES itu sendiri merupakan algoritma cryptographic yang dapat digunakan untuk mengamankan data dengan substitusi, enkripsi blok mutasi, dan putaran ganda dalam proses enkripsi dan dekripsi setiap blok [4].

Pada tahap awal, aplikasi ini dirancang untuk dioperasikan secara lokal di lokasi kedai saja. Ini memungkinkan pengelolaan data secara real-time dan sinkronisasi data yang lebih baik, serta dapat mengurangi ancaman serangan dari lokasi eksternal. Penerapan aplikasi RMS ini diharapkan tidak hanya meningkatkan efisiensi operasional tetapi juga memberikan rasa aman dalam mengelola informasi sensitif. Penggunaan kriptografi AES-256-GCM merupakan langkah penting dalam memastikan bahwa data transaksi tetap aman dan tidak dapat diakses oleh pihak yang tidak berwenang. AES-256-GCM digunakan karena tingkat keamanannya yang tinggi dengan panjang kunci 256-bit dan jumlah putaran enkripsi yang berulang. Mode Galois/Counter Mode (GCM) menyediakan otentikasi data yang memastikan integritas pesan selain enkripsi. Kombinasi ini memberikan perlindungan menyeluruh terhadap ancaman cyber, menjadikannya pilihan ideal untuk keamanan kriptografi saat ini.

Dengan demikian tujuan dari pengembangan sistem ini adalah untuk meningkatkan efisiensi operasional dan keamanan data transaksi di Kedai Talok Fried Chicken Baciro. Dengan adanya aplikasi RMS yang terintegrasi dan dilengkapi dengan kriptografi AES-256-GCM, diharapkan proses pengelolaan pesanan dan transaksi keuangan menjadi lebih efisien dan

terjamin keamanannya. Selain itu, aplikasi ini juga berfungsi untuk memberikan pemilik kedai kontrol penuh terhadap operasional mereka dan mengurangi ketergantungan pada platform pihak ketiga. Diharapkan usaha kuliner ini dapat berkembang lebih baik dan menjadi contoh bagi industri lainnya dalam mengadopsi teknologi untuk meningkatkan kinerja dan keamanan operasional.

## **1.2 Rumusan Masalah**

Diterapkannya keamanan kriptografi pada aplikasi RMS, dikarenakan sebelumnya Kedai Talok Fried Chicken Baciro masih menggunakan aplikasi pihak ketiga yang tingkat keamanannya sangat rendah. Pemilik (Admin/Owner) kedai tidak memiliki akses langsung untuk meninjau laporan dan data transaksi penjualan. Penerapan aplikasi Restaurant Management System (RMS) ini diharapkan dapat memberikan hak akses dan kontrol penuh kepada pemilik kedai, meningkatkan efisiensi operasional kedai, serta dapat melindungi data transaksi dengan keamanan kriptografi dari potensi ancaman manipulasi data.

## **1.3 Batasan Masalah**

1. Metode kriptografi yang digunakan dalam aplikasi RMS ini adalah Advanced Encryption Standard (AES) dengan panjang kunci 256-bit dengan mode Galois/Counter Mode (GCM). Metode ini dipilih karena keandalannya dalam memberikan keamanan data yang baik.
2. Aplikasi RMS (Restaurant Management System) ini dirancang dengan kontrol akses yang ketat, di mana hanya admin (owner/pemilik), pegawai (kasir & pelayan), dan bagian dapur yang memiliki hak akses untuk masuk dan menggunakan aplikasi ini. Customer tidak memiliki akses untuk masuk ke aplikasi ini, di karenakan aplikasi RMS ini dibuat hanya untuk lingkungan internal saja belum dikembangkan untuk lingkungan luas atau tingkat profesional.
3. Metode pengembangan software yang dipakai adalah RAD (Rapid Application Development). RAD dipilih karena tahapannya terstruktur dan mudah dipahami, serta dapat dilakukan dalam waktu yang relatif cepat dan siklus yang pendek. Sangat cocok untuk pengembangan aplikasi dengan skala kecil.
4. Aplikasi RMS ini dibatasi dengan hanya dapat diakses secara offline atau lokal, untuk meminimalisir ancaman dan serangan dari luar. Karena aplikasi RMS ini juga dikhususkan untuk lingkungan kedai saja (internal) bukan untuk jangkauan luas (eksternal).

#### **1.4 Tujuan Penelitian**

Penelitian ini bertujuan untuk mengembangkan aplikasi Restaurant Management System (RMS) dengan fitur kriptografi di Kedai Talok Fried Chicken Baciro agar tidak memiliki ketergantungan pada aplikasi pihak ketiga seperti Shopee dan GoFood, yang rawan terhadap serangan digital. Dengan aplikasi RMS, diharapkan operasional kedai dapat dikelola secara mandiri dan efisien. Aplikasi ini menggunakan keamanan kriptografi AES-256-GCM untuk menjaga kerahasiaan dan integritas data transaksi, meningkatkan keamanan, dan mengurangi risiko manipulasi serta pencurian informasi.

#### **1.5 Manfaat Penelitian**

Penelitian ini diharapkan dapat meningkatkan keamanan data di Kedai Talok Fried Chicken Baciro melalui penerapan kriptografi AES-256-GCM pada aplikasi RMS, terutama untuk melindungi data transaksi dari cybercrime dan manipulasi. Aplikasi RMS akan mengelola pesanan, stok, dan transaksi keuangan lebih efisien, mengurangi ketergantungan pada aplikasi pihak ketiga, dan mengoptimalkan kinerja pegawai. Pemilik kedai dapat memiliki hak akses penuh terhadap sistem pemesanan tanpa berbagi biaya komisi dengan Shopee dan GoFood. Sistem yang terintegrasi dan aman, membuat layanan pelanggan akan lebih baik, dan meningkatkan kepuasan serta loyalitas pelanggan.

## **BAB V**

### **PENUTUP**

#### **5.1 Kesimpulan**

Mencakup semua bahasan diatas, maka dapat disimpulkan bahwa penerapan Kriptografi AES-256-GCM pada aplikasi RMS Kedai Talok Fried Chicken Baciro telah berhasil dilakukan. Hasil penelitiannya adalah data transaksi dan juga data pribadi pelanggan yang bersifat sensitif seperti nama pelanggan, nohp pelanggan, dan alamat pelanggan dapat di enkripsi dan juga di dekripsi secara otomatis serta tersimpan secara otomatis juga di database, kemudian untuk keys enkripsi dan dekripsinya tidak disimpan di publik html atau di database, melainkan disimpan dalam fungsi environment variable atau server sendiri demi menjaga integritas data keys dari ancaman serangan. Dengan adanya Aplikasi RMS berbasis Kriptografi ini, memungkinkan manipulasi data dapat dikurangi, dan juga pemilik atau owner Kedai Talok Fried Chicken Baciro dapat sepenuhnya mengakses serta mengelola data transaksi pelanggannya dengan aman tanpa harus bergantung kepada aplikasi pihak ketiga. Selain penerapan dan implementasi, dalam penelitian ini juga dilakukan pengujian dan evaluasi, untuk menganalisis apakah penerapan Kriptografi pada aplikasi RMS sudah benar-benar berhasil dilakukan atau masih ditemukan kerentanan dan potensi serangan yang mengancam keamanan data. Terdapat dua pengujian dan evaluasi, yaitu pada aplikasi RMS berbasis Kriptografi dan aplikasi RMS tanpa Kriptografi. Hasil pengujian dan evaluasi memperlihatkan aplikasi RMS berbasis Kriptografi lebih sedikit ditemukan kerentanan potensi serangannya daripada aplikasi RMS tanpa Kriptografi.

#### **5.2 Saran**

Dalam penelitian ini masih terdapat beberapa kekurangan, diantaranya adalah Aplikasi RMS yang dibuat belum dikembangkan untuk jangkauan luas atau profesional. Akses usernya masih terbatas hanya untuk lingkungan kedai saja, pelanggan atau customer tidak bisa mengaksesnya. Kemudian untuk penerapan kriptografi dengan model AES-256-GCM secara umum sudah berhasil dilakukan, namun setelah dilakukan pengujian dan evaluasi masih terdapat beberapa kerentanan dan ancaman terhadap keamanan data. Maka dengan itu, peneliti berharap untuk penelitian selanjutnya yang mempunyai kesamaan tema bahasan dengan penelitian ini, bisa lebih baik lagi dalam memilih model kriptografi yang tepat dan kompleks agar nantinya potensi serangan atau ancaman terhadap keamanan data bisa lebih berkurang dan bisa lebih minimal lagi.

## DAFTAR PUSTAKA

- [1] F. Jingga and N. Limantara, "Pembangunan Model Restaurant Management System," *ComTech*, vol. 5, no. 2, p. 973, Dec. 2014, doi: 10.21512/comtech.v5i2.2348.
- [2] R. Mulud Muchamad, A. Asriyanik, and A. Pambudi, "IMPLEMENTASI ALGORITMA ADVANCED ENCRYPTION STANDARD (AES) UNTUK MENGENKRIPSI DATASTORE PADA APLIKASI BERBASIS ANDROID," *Mnemonic*, vol. 6, no. 1, pp. 55–64, May 2023, doi: 10.36040/mnemonic.v6i1.5889.
- [3] H. Prilandi and D. Kusumaningsih, "PENERAPAN APLIKASI KRIPTOGRAFI DENGAN ALGORITMA ADVANCED ENCRYPTION STANDARD PADA PERUSAHAAN PT CAHAYA TELEVISI INDONESIA," 2022.
- [4] F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard," *JIM*, vol. 10, no. 1, p. 20, Jun. 2016, doi: 10.30872/jim.v10i1.23.
- [5] M. H. Ibrahim, S. Mulyati, and J. C. Chandra, "IMPLEMENTASI ALGORITMA ADVANCED ENCRYPTION STANDARD 128 (AES 128) BERBASIS WEB PADA KEDAI KOPI NGOPIYUKA!," vol. 2, 2023.
- [6] H. D. Novianti and Ahmad Tri Hidayat, "IMPLEMENTASI KRIPTOGRAFI ADVANCED ENCRYPTION STANDARD 128 BIT DALAM PENGAMANAN DATA KEUANGAN KAS: (Studi Kasus: Masjid Al-Ikhlas Trini Sleman D.I.Yogyakarta)," *jukomtek*, pp. 27–34, Jan. 2023, doi: 10.58290/jukomtek.v1i2.51.
- [7] M. R. Andriyanto and P. Sukmasetya, "Penerapan Algoritma Advanced Encryption Standard (AES) Untuk Keamanan Data Transaksi Pada Sistem E-Marketplace," *JoSYC*, vol. 4, no. 1, pp. 179–187, Dec. 2022, doi: 10.47065/josyc.v4i1.2451.
- [8] B. T. Mahardika and M. R. Alfian, "PENERAPAN ALGORITMA KRIPTOGRAFI UNTUK PENGAMANAN DOKUMEN TRANSAKSI DENGAN METODE RIVEST SHAMIR ADLEMAN," no. 1, 2022.
- [9] F. A. Sitorus and N. B. Nugroho, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Bit Untuk Keamanan Data Transaksi Penjualan Pada PT. MITSUBISHI ELECTRIC INDONESIA.," 2020.
- [10] I. Afrianto and N. Taliasih, "Sistem Keamanan Basis Data Klien P.T. Infokes Menggunakan Kriptografi Kombinasi RC4 Dan Base64," *TEKNOSI*, vol. 6, no. 1, pp. 9–18, May 2020, doi: 10.25077/TEKNOSI.v6i1.2020.9-18.
- [11] E. Sutinah, I. Alfarobi, and A. Setiawan, "Metode Rapid Application Development dalam Pembuatan Sistem Informasi Pemenuhan SDM pada Perusahaan Outsourcing," vol. 5, 2021.
- [12] D. Hariyanto, R. Sastra, and F. E. Putri, "Implementasi Metode Rapid Application Development Pada Sistem Informasi Perpustakaan," vol. 13, no. 1, 2021.
- [13] A. Rahman, "Rapid Application Development Sistem Pembelajaran Daring Berbasis Android," *INTECH*, vol. 1, no. 2, pp. 20–25, Nov. 2020, doi: 10.54895/intech.v1i2.639.
- [14] R. Febrianto and S. Waluyo, "Implementasi Algoritme Kriptografi Advanced Encryption Standard (AES-256) Untuk Mengamankan Database Penilaian Karyawan Pada KJPP NDR," *Bit*, vol. 20, no. 1, p. 44, Apr. 2023, doi: 10.36080/bit.v20i1.2223.
- [15] R. Tullah, M. I. Dzulhaq, and Y. Setiawan, "Perancangan Aplikasi Kriptografi File Dengan Metode Algoritma Advanced Encryption Standard (AES)," vol. 6, no. 2, 2023.

- [16] W. Riyadi, “KRIPTOGRAFI SYMMETRIC-KEY CRYPTOSYSTEM DENGAN METODE AES (ADVANCED ENCRYPTION STANDARD) 256bit,” 2016.
- [17] B. E. Widodo and A. S. Purnomo, “IMPLEMENTASI ADVANCED ENCRYPTION STANDARD PADA ENKRIPSI DAN DEKRIPSI DOKUMEN RAHASIA DITINTELKAM POLDA DIY,” *Jurnal Teknik Informatika*, vol. 1, no. 2, pp. 69–77, Dec. 2020, doi: 10.20884/1.jutif.2020.1.2.21.
- [18] I. Hajar, “Pengamanan Arsip dengan Algoritma Enkripsi AES-256 untuk Web App E-Arsip Yayasan Universitas Islam Sumatera Utara,” *hello world j. ilmu komp'ût.*, vol. 1, no. 2, pp. 76–89, Jul. 2022, doi: 10.56211/helloworld.v1i2.13.
- [19] G. W. Bhaudhayana and I. M. Widiartha, “IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES 256 DAN METODE STEGANOGRAFI LSB PADA GAMBAR BITMAP”.
- [20] D. A. McGrew, S. Jose, and J. Viega, “The Galois/Counter Mode of Operation (GCM),” 2024.
- [21] Universitas Methodist Indonesia, J. Jamaluddin, N. F. Saragih, R. J. Simamora, R. Siringoringo, and E. N. Purba, “KONSEP PENGAMANAN VIDEO CONFERENCE DENGAN ENKRIPSI AES-GCM PADA APLIKASI ZOOM,” *jmika*, vol. 4, no. 2, pp. 109–113, Oct. 2021, doi: 10.46880/jmika.Vol4No2.pp109-113.
- [22] A. F. Hasibuan and D. Handoko, “Analisis Keretakan Website Dengan Aplikasi Owasp Zap,” vol. 2, 2023.