# BAB 1
# PENDAHULUAN

## 1.1 Latar Belakang

Perkembangan teknologi dan internet membuat belanja online semakin mudah dan jadi kebiasaan banyak orang. Marketplace besar seperti Shopee, Tokopedia, dan TikTok Shop sudah terkenal, banyak promo, dan dipercaya jutaan orang. Tapi di balik kemudahan itu, masalah kebocoran data pelanggan masih sering terjadi.

Salah satu contoh nyata pentingnya keamanan data di dunia *e-commerce* terjadi pada Mei 2020. Saat itu, Tokopedia — salah satu platform belanja online terbesar di Indonesia — mengalami kebocoran data besar. Sekitar 91 juta data pengguna, seperti nama lengkap, email, nomor telepon, dan kata sandi (meski sudah diacak) bocor dan dijual di forum gelap (*dark web*). Kejadian ini membuat banyak pengguna merasa khawatir dan kehilangan kepercayaan. Kasus ini menunjukkan bahwa menjaga keamanan data bukan hanya soal teknis, tapi juga soal menjaga kepercayaan pelanggan dan kelangsungan bisnis.

Selain itu, masih banyak kasus penipuan COD palsu. Data nama, alamat, dan nomor telepon pelanggan yang bocor sering dimanfaatkan orang tidak bertanggung jawab. Contohnya, pembeli didatangi kurir yang mengaku membawa paket padahal tidak pernah dipesan. Karena data sudah bocor, banyak orang lengah dan langsung membayar karena mengira paket itu untuk anggota keluarga mereka.

Berdasarkan penelitian (Muttaqin & Indonesia, 2024) , penerapan algoritma *Advanced Encryption Standard* (AES)-128 terbukti bisa meningkatkan keamanan transaksi dan data pengguna dalam platform *e-commerce*. Hal ini juga didukung oleh studi (Mustika, 2020) yang menjelaskan bahwa implementasi enkripsi AES di sistem login dan penyimpanan data pengguna bisa secara signifikan mengurangi risiko kebocoran informasi. Dengan makin tingginya serangan siber, teknologi enkripsi bukan lagi pilihan tambahan, tetapi sudah jadi solusi mendesak yang harus diterapkan pada sistem informasi *e-commerce*.

Melihat masalah ini, Toko Gals Collection ingin membangun platform *e-commerce* sendiri dengan fokus utama menjaga kepercayaan dan loyalitas

pelanggan. Website ini akan menerapkan enkripsi data menggunakan AES, sehingga data penting seperti nama, alamat, nomor telepon, dan detail pesanan akan diamankan. Hanya pihak yang benar-benar berwenang yang bisa membuka data ini. Informasi yang dilihat penjual juga akan dibatasi hanya sebatas yang diperlukan untuk pengiriman barang.

Selain menjaga keamanan data, memiliki website sendiri juga memberi keuntungan lebih besar bagi Toko Gals Collection. Dengan platform sendiri, toko tidak perlu membayar biaya komisi marketplace yang bisa mencapai 5–15% per transaksi. Keuntungan ini bisa digunakan untuk meningkatkan layanan, promo khusus, dan program loyalitas agar pembeli betah belanja langsung di website.

Walaupun produk yang dijual Toko Gals Collection tidak jauh berbeda dengan produk global yang banyak dijual di pasaran, jaminan perlindungan data dan rasa aman berbelanja akan menjadi nilai tambah utama. Dengan strategi promosi digital seperti iklan di media sosial, kerja sama dengan influencer, dan penawaran khusus untuk pelanggan setia, diharapkan website ini dapat menjangkau pasar lebih luas — tidak hanya teman dekat saja, tetapi juga pembeli dari berbagai wilayah.

Dengan cara ini, Toko Gals Collection ingin membangun platform belanja online yang aman, terpercaya, dan mendukung loyalitas pelanggan, supaya tidak ada lagi rasa khawatir berbelanja karena data bocor atau disalahgunakan.

## 1.2 Perumusan Masalah

Keamanan dalam transaksi *e-commerce* merupakan aspek krusial yang perlu diperhatikan, terutama dalam melindungi data pelanggan dari ancaman peretasan dan penyalahgunaan informasi. Toko Gals Collection sebagai *platform e-commerce* yang sedang dikembangkan membutuhkan sistem keamanan yang dapat menjaga kerahasiaan serta integritas data transaksi.

Beberapa permasalahan yang menjadi fokus dalam proyek ini adalah:

1) Bagaimana cara mengimplementasikan enkripsi data menggunakan metode AES agar transaksi pada Toko Gals Collection lebih aman?
2) Bagaimana sistem dapat memastikan bahwa data pelanggan dan transaksi tidak mudah diakses oleh pihak yang tidak berwenang?

## 1.3 Batasan Masalah

Agar ruang lingkup penelitian tidak terlalu luas, batasan masalah yang diterapkan adalah sebagai berikut:

1) Sistem yang dikembangkan hanya berfokus pada keamanan data transaksi dan informasi pelanggan menggunakan metode enkripsi AES.
2) Platform *e-commerce* yang dibuat hanya digunakan untuk Toko Gals Collection dan tidak mencakup integrasi dengan marketplace lain.
3) Penelitian ini hanya membahas implementasi enkripsi AES pada proses penyimpanan ke dalam database, tanpa mencakup aspek keamanan lain seperti firewall atau sistem deteksi intrusi (IDS).

## 1.4 Tujuan dan Manfaat

### *1.4.1 Tujuan*

Adapun Tujuan dalam pembuatan proyek akhir ini adalah:

1) Mengembangkan sistem informasi *e-commerce* yang aman dengan menerapkan metode enkripsi AES untuk melindungi data transaksi pelanggan di Toko Gals Collection.
2) Memastikan bahwa informasi pelanggan, seperti data pribadi dan riwayat transaksi, tidak dapat diakses oleh pihak yang tidak berwenang.
3) Menerapkan enkripsi sebagai langkah utama untuk menjaga kerahasiaan dan integritas data pelanggan selama proses penyimpanan maupun pengiriman data.

### *1.4.2 Manfaat*

Hasil dari penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1) Memberikan solusi keamanan berbasis enkripsi AES untuk transaksi online, sehingga mengurangi risiko pencurian data oleh pihak yang tidak bertanggung jawab.
2) Menyediakan platform *e-commerce* yang lebih aman bagi pelanggan, yang dapat meningkatkan loyalitas dan kredibilitas bisnis.
3) Mempermudah pengelolaan transaksi secara efisien dengan tetap menjaga privasi dan keamanan data pelanggan.

4) Menjadi referensi dan acuan bagi pengembang lain dalam membangun sistem *e-commerce* dengan tingkat keamanan yang lebih baik.

# BAB 2
# TINJAUAN PUSTAKA

## 2.1 Landasan Teori

Landasan teori merupakan dasar konseptual yang digunakan sebagai acuan dalam pelaksanaan penelitian ini. Pada bagian ini dijelaskan teori-teori yang berkaitan dengan pengembangan sistem *e-commerce*, keamanan transaksi, algoritma enkripsi AES-128, SQL Injection, serta teknologi pendukung lainnya yang digunakan dalam perancangan dan implementasi website Gals Collection. Teori-teori tersebut menjadi dasar dalam menganalisis, merancang, mengimplementasikan, dan mengevaluasi sistem yang dikembangkan.

### *2.1.1 E-Commerce*

*E-commerce* atau electronic commerce merupakan kegiatan jual beli barang atau jasa melalui jaringan internet. *E-commerce* didefinisikan sebagai penggunaan internet, web, dan aplikasi *mobile* untuk melakukan transaksi bisnis antara organisasi dan individu. *E-commerce* memberi beberapa manfaat, di antaranya:

1) Memperluas jangkauan pasar tanpa batasan geografis
2) Beroperasi 24 jam sehari, 7 hari seminggu
3) Mengurangi biaya operasional dibandingkan toko fisik
4) Memudahkan pelacakan dan analisis perilaku konsumen
5) Meningkatkan efisiensi distribusi produk

Terdapat beberapa jenis *e-commerce* berdasarkan pihak yang terlibat dalam transaksi, yaitu:

1) B2C (*Business to Consumer*): Transaksi antara bisnis dengan konsumen akhir
2) B2B (*Business to Business*): Transaksi antara satu bisnis dengan bisnis lainnya
3) C2C (*Consumer to Consumer*): Transaksi antara konsumen dengan konsumen lainnya
4) C2B (*Consumer to Business*): Transaksi di mana konsumen menawarkan produk/jasa kepada bisnis

Toko Gals Collection termasuk dalam kategori B2C *e-commerce*, di mana transaksi dilakukan antara bisnis (toko) dengan konsumen akhir.

### *2.1.2 Toko Gals Collection*

Toko Gals Collection adalah sebuah usaha ritel yang bergerak di bidang penjualan berbagai produk fashion, aksesoris, dan kebutuhan gaya hidup lainnya. Toko ini berfokus pada penyediaan produk dengan harga terjangkau namun tetap mengutamakan kualitas dan keaslian barang.

Saat ini, Toko Gals Collection melayani pelanggan melalui toko fisik dan media sosial, seperti Instagram dan *WhatsApp*. Namun, sistem penjualannya masih dilakukan secara manual, mulai dari pencatatan stok barang, pengelolaan data pelanggan, hingga transaksi pembayaran. Hal ini sering menimbulkan beberapa kendala, seperti risiko kehilangan data, kesalahan pencatatan, dan lambatnya proses transaksi.

Untuk itu, Toko Gals Collection berencana mengembangkan sistem *e-commerce* mandiri berbasis web. Sistem ini bertujuan untuk mempermudah pelanggan dalam melihat katalog produk, melakukan pemesanan, serta mempermudah pihak toko dalam mengelola data transaksi. Selain itu, sistem juga akan dilengkapi fitur keamanan berupa enkripsi data menggunakan metode AES (*Advanced Encryption Standard*) untuk menjaga kerahasiaan data pelanggan dan transaksi.

Dengan adanya pengembangan sistem ini, diharapkan proses bisnis Toko Gals Collection dapat berjalan lebih cepat, aman, dan efisien, serta mampu meningkatkan kepuasan pelanggan.


Gambar *2.1* Toko *Gals Collection*

### *2.1.3 Keamanan Transaksi E-Commerce*

Keamanan transaksi dalam *e-commerce* merupakan aspek krusial yang menentukan kepercayaan pelanggan. Terdapat beberapa ancaman keamanan yang perlu dihadapi oleh sistem *e-commerce*, di antaranya:

1) *Data Breach*: Pencurian data pelanggan dari database sistem
2) *Man-in-the-Middle Attack*: Penyusupan dalam komunikasi antara dua pihak
3) *Phishing*: Penipuan untuk mendapatkan informasi sensitif pengguna
4) *SQL Injection*: Serangan yang memanfaatkan kerentanan dalam kode aplikasi
5) *Cross-Site Scripting (XSS)*: Penyisipan kode berbahaya ke dalam situs web

Untuk mengatasi ancaman tersebut, diperlukan beberapa mekanisme keamanan, salah satunya adalah enkripsi data. Enkripsi merupakan proses konversi data asli (*plaintext*) menjadi bentuk yang tidak dapat dibaca (*ciphertext*) menggunakan algoritma tertentu dan kunci enkripsi.

### *2.1.4 Enkripsi Data*

Menurut Suyanto. (2012) , enkripsi merupakan suatu proses pengamanan data dengan cara mengubah data asli (*plaintext*) menjadi data yang tidak dapat dibaca (*ciphertext*) tanpa kunci tertentu. Tujuan dari proses ini adalah untuk menjaga kerahasiaan data agar tidak disalahgunakan oleh pihak yang tidak berwenang, khususnya saat data berpindah antar sistem atau disimpan dalam media penyimpanan yang rentan diakses oleh pihak luar.

Enkripsi menjadi semakin penting seiring dengan berkembangnya penggunaan aplikasi komputer dalam organisasi atau perusahaan, di mana banyak aplikasi yang membutuhkan pertukaran data antar sistem. Dalam kondisi seperti ini, risiko penyalahgunaan data sangat tinggi, sehingga diperlukan suatu metode untuk mengamankan data tersebut. Salah satu metode yang terbukti efektif adalah penggunaan teknik enkripsi.

Enkripsi sendiri merupakan bagian dari ilmu kriptografi, yaitu ilmu yang mempelajari teknik-teknik matematis untuk menjaga keamanan informasi dari segi kerahasiaan, keaslian, integritas, serta autentikasi data (Suyanto, 2012). Dalam penerapannya, terdapat dua jenis enkripsi yang umum digunakan, yaitu:

1) Enkripsi Simetris (*Symmetric Encryption*), yaitu metode enkripsi yang

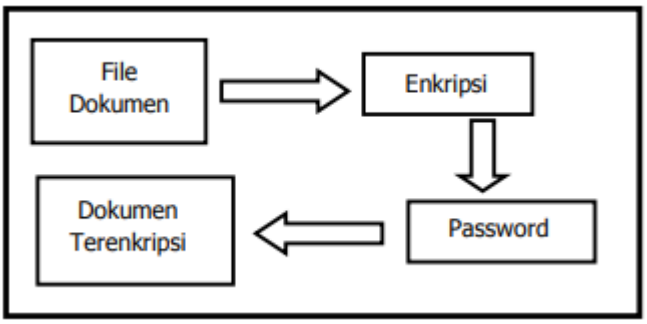
menggunakan satu kunci yang sama untuk proses enkripsi dan dekripsi.

2) Enkripsi Asimetris (Asymmetric Encryption), yaitu metode enkripsi yang menggunakan sepasang kunci, yakni kunci publik untuk enkripsi dan kunci privat untuk dekripsi.

Dalam penelitiannya, Suyanto menggunakan metode enkripsi simetris dengan algoritma Substitution Cipher, yaitu dengan cara menggantikan setiap karakter dari plaintext ke karakter lain berdasarkan nilai pergeseran tertentu (Cn). Nilai Cn ini dapat diatur sesuai kebutuhan pengguna.

Lebih lanjut, hasil dari proses enkripsi dapat dikonversi ke dalam format XML agar dapat dibaca oleh berbagai jenis database meskipun berbeda platform. Format XML ini bersifat lintas platform dan memungkinkan pertukaran data yang lebih fleksibel antar aplikasi (Suyanto, 2012).

Dengan demikian, dapat disimpulkan bahwa enkripsi merupakan solusi penting dalam menjaga keamanan data, terutama dalam proses pertukaran dan penyimpanan data antar sistem berbasis komputer. Secara umum, proses enkripsi dimulai dengan mengubah data asli (plaintext) menjadi data terenkripsi (ciphertext) menggunakan suatu algoritma dan kunci enkripsi. Selanjutnya, data tersebut dapat dikembalikan ke bentuk semula (plaintext) menggunakan kunci yang sesuai melalui proses dekripsi. Alur proses enkripsi dan dekripsi tersebut ditunjukkan pada Gambar 2.2 (Kilat, 2018) .




Gambar 2.2 Cara kerja enkripsi

### *2.1.5 Advanced Encryption Standard (AES)*

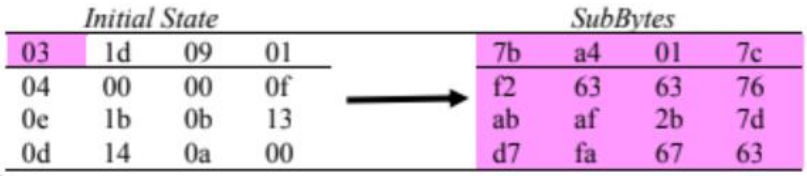
*Advanced Encryption Standard* (AES) adalah algoritma enkripsi simetris yang ditetapkan sebagai standar oleh National Institute of Standards and Technology (NIST) pada tahun 2001. AES menggantikan algoritma Data

Encryption Standard (DES) yang sudah dianggap tidak aman lagi. AES menggunakan sistem block cipher dengan ukuran blok tetap sebesar 128 bit dan ukuran kunci yang bervariasi yaitu 128, 192, atau 256 bit.

Proses enkripsi AES terdiri dari beberapa tahap utama:

1) SubBytes: Substitusi non-linear dari setiap byte menggunakan tabel S-box.

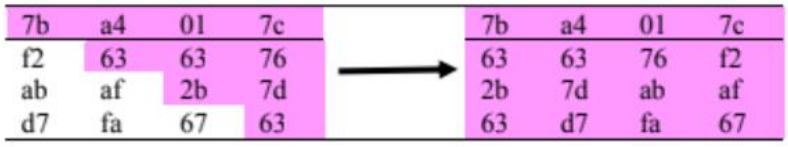
   Tahap SubBytes merupakan proses substitusi non-linear pada setiap byte dalam state array menggunakan tabel Substitution Box (S-box). Tujuan dari tahap ini adalah mengganti setiap nilai byte dengan nilai baru berdasarkan tabel S-box sehingga meningkatkan tingkat keamanan algoritma AES. Ilustrasi proses SubBytes dapat dilihat pada Gambar 2.3 (Mustika, 2020).




Gambar 2.3 Proses *SubBytes*

2) ShiftRows: Pergeseran baris-baris dalam state array.

   Tahap ShiftRows merupakan proses pergeseran setiap baris pada state array. Baris pertama tidak mengalami pergeseran, sedangkan baris kedua, ketiga, dan keempat digeser ke kiri dengan jumlah yang berbeda-beda. Pergeseran ini bertujuan untuk menyebarkan hasil substitusi sehingga meningkatkan tingkat kerumitan proses enkripsi. Proses ShiftRows ditunjukkan pada Gambar 2.4 (Mustika, 2020).




Gambar 2.4 Proses *ShiftRows*

3) MixColumns: Transformasi linear mencampur kolom-kolom dalam state array.

   Tahap MixColumns melakukan transformasi linear pada setiap kolom dalam state array. Proses ini mengombinasikan setiap byte pada kolom menggunakan operasi matematika pada medan hingga (Galois Field) sehingga menghasilkan nilai baru yang semakin sulit diprediksi. Ilustrasi proses MixColumns dapat dilihat pada Gambar 2.5 (Mustika, 2020).

$$\begin{bmatrix} r0 \\ r1 \\ r2 \\ r3 \end{bmatrix} = \begin{bmatrix} 2\,3\,1\,1 \\ 1\,2\,3\,1 \\ 1\,1\,2\,3 \\ 3\,1\,1\,2 \end{bmatrix} \begin{bmatrix} a0 \\ a1 \\ a2 \\ a3 \end{bmatrix}$$

Dimana r0, r1, r2 dan r3 adalah hasil setelah transformasi. a0 - a3 dapat diperoleh dari matriks setelah data mengalami proses substitusi dalam *Sbox*. Untuk memperoleh nilai r0, rumusnya seperti dibawah ini :

$$r0 = \{02.a0\} xor \{03.a1\} xor \{01.02\} xor \{01.03\}$$
$$r1 = \{01.a0\} xor \{02.a1\} xor \{03.02\} xor \{01.03\}$$
$$r2 = \{01.a0\} xor \{01.a1\} xor \{02.02\} xor \{03.03\}$$
$$r3 = \{03.a0\} xor \{01.a1\} xor \{01.02\} xor \{03.03\}$$

Gambar 2.5 Proses *MixColumns*

4) AddRoundKey: Penambahan round key ke state array.

Tahap AddRoundKey merupakan proses menggabungkan state array dengan round key menggunakan operasi XOR. Tahap ini dilakukan pada setiap putaran algoritma AES sehingga hanya pihak yang memiliki kunci yang benar yang dapat melakukan proses dekripsi. Proses AddRoundKey ditunjukkan pada Gambar 2.6 (Mustika, 2020).

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 68 | 6f | 6b | 72 | | 6b | 72 | 62 | 73 | | 03 | 1d | 09 | 01 |
| 65 | 61 | 61 | 6e | ⊕ | 61 | 61 | 61 | 61 | = | 04 | 00 | 00 | 0f |
| 6c | 70 | 62 | 79 | | 62 | 6b | 69 | 6a | | 0e | 1b | 0b | 13 |
| 6c | 61 | 61 | 61 | | 61 | 75 | 6b | 61 | | 0d | 14 | 0a | 00 |
| *Plaintext* | | | | | *Key* | | | | | Hasil *AddRoundKey* | | | |

Gambar 2.6 Proses *AddRoundKey*

Jumlah putaran (round) dalam AES bergantung pada panjang kunci yang digunakan:

1) AES-128: 10 putaran
2) AES-192: 12 putaran
3) AES-256: 14 putaran

Kekuatan keamanan AES terletak pada kompleksitas algoritma dan panjang kunci yang digunakan. Untuk AES-128, terdapat $2^{128}$ kemungkinan kunci, yang secara praktis tidak mungkin dipecahkan dengan teknologi komputasi saat ini melalui metode brute force. Perbedaan konfigurasi AES berdasarkan panjang kunci, jumlah putaran (round), serta ukuran sub-key yang dihasilkan dapat dilihat pada Gambar 2.7 (Daoud et al., 2019). Semakin besar ukuran kunci yang digunakan, maka semakin banyak jumlah putaran enkripsi yang dilakukan sehingga tingkat keamanan algoritma juga semakin meningkat. Namun, pada penelitian ini digunakan AES-128 karena telah memberikan tingkat keamanan yang tinggi dengan proses komputasi yang lebih efisien dibandingkan AES-192 maupun AES-256.

| AES configuration | Rounds | Key size (bits) | Sub-key size (bytes) |
|---|---|---|---|
| AES-128 | 10 | 128 | 176 |
| AES-192 | 12 | 192 | 208 |
| AES-256 | 14 | 256 | 240 |

Gambar 2.7 *AES Design*

### *2.1.6 Metode Waterfall*

Metode Waterfall adalah salah satu model System Development Life Cycle (SDLC) yang sering digunakan dalam pengembangan sistem informasi atau perangkat lunak. Menurut (Wahid, 2020) , model Waterfall menggunakan pendekatan yang sistematis dan berurutan, di mana setiap tahap harus diselesaikan sepenuhnya sebelum melanjutkan ke tahap berikutnya.

Model ini pertama kali diperkenalkan oleh Winston Royce sekitar tahun 1970. Karena tahapan yang dilalui harus dijalankan secara berurutan dari awal hingga akhir, model ini sering disebut juga dengan istilah Linear Sequential Model (Classic Life Cycle). Dalam praktiknya, metode Waterfall cocok digunakan pada proyek pembuatan sistem baru maupun pengembangan sistem berskala besar di mana kebutuhan pengguna relatif jelas sejak awal.

Tahapan Metode Waterfall (Wahid, 2020):

1) Requirement

Tahap ini fokus pada komunikasi antara pengembang dengan pengguna untuk memahami kebutuhan perangkat lunak. Data dapat dikumpulkan melalui wawancara, survei, atau diskusi. Hasilnya dianalisis untuk menentukan spesifikasi kebutuhan secara detail.

2) Design

Pengembang merancang sistem berdasarkan hasil analisis kebutuhan. Desain ini mencakup arsitektur sistem, spesifikasi perangkat keras, perangkat lunak, struktur basis data, dan antarmuka pengguna.

3) Implementation

Pada tahap ini, desain diubah menjadi kode program. Sistem dikembangkan menjadi unit-unit kecil yang kemudian diintegrasikan. Tiap unit diuji secara mandiri melalui unit testing.

4) Verification

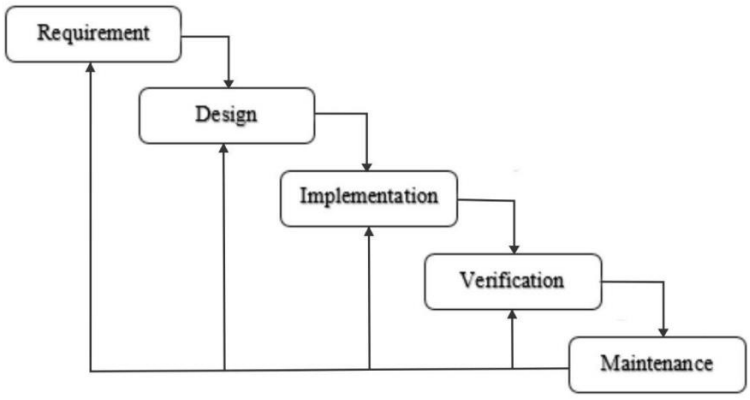
Tahap verifikasi dilakukan untuk memastikan bahwa sistem memenuhi semua kebutuhan yang telah ditentukan. Pengujian meliputi unit testing, system testing, dan acceptance testing bersama pengguna untuk memastikan bahwa sistem berfungsi sesuai harapan.

5) Maintenance

Setelah sistem diimplementasikan, tahap pemeliharaan dilakukan untuk memperbaiki kesalahan yang tidak terdeteksi sebelumnya dan menyesuaikan sistem dengan kebutuhan baru.

Wahid (2020) menyatakan bahwa kelebihan metode Waterfall adalah kualitas sistem yang dihasilkan baik karena pelaksanaannya bertahap, dokumentasi terorganisir dengan rapi, dan prosesnya meminimalisir kesalahan berulang. Namun, kekurangannya adalah proses pengembangan memerlukan waktu relatif lama dan biaya lebih besar. Selain itu, perubahan kebutuhan mendadak sulit diterapkan karena model ini jarang mendukung iterasi mundur ke tahap sebelumnya.

Dengan pendekatan bertahap dan dokumentasi terstruktur, metode Waterfall sesuai digunakan pada pengembangan sistem informasi *e-commerce* Toko Gals Collection, untuk memastikan penerapan enkripsi AES terintegrasi secara rapi pada setiap tahap pengembangan. Tahapan metode Waterfall yang digunakan dalam penelitian ini ditunjukkan pada Gambar 2.8 (Wahid, 2020).




Gambar 2.8 Metode *Waterfall*

### *2.1.7 Database*

Database adalah kumpulan data yang disusun secara terstruktur sehingga

dapat disimpan, dikelola, dan diakses dengan mudah menggunakan sistem manajemen basis data (Database Management System atau DBMS). Database digunakan untuk menyimpan berbagai informasi yang dibutuhkan oleh suatu aplikasi, seperti data pengguna, data produk, transaksi, dan informasi lainnya.

Pada sistem *e-commerce*, database memiliki peran penting karena seluruh aktivitas pengguna, seperti proses registrasi, login, pemesanan, hingga pembayaran akan disimpan ke dalam database. Oleh karena itu, keamanan database harus menjadi perhatian utama agar data yang tersimpan tidak mudah diakses atau disalahgunakan oleh pihak yang tidak berwenang.

Pada penelitian ini, MySQL digunakan sebagai sistem manajemen basis data (Database Management System atau DBMS) untuk menyimpan seluruh data pada website Gals Collection. Data disimpan ke dalam beberapa tabel yang saling berhubungan, di mana setiap tabel terdiri atas beberapa record (baris data) dan field (kolom data). Struktur dasar penyimpanan data pada database ditunjukkan pada Gambar 2.9 (Helilintar, 2017).


Gambar 2.9 Struktur *Database*

### *2.1.8 TLS*

Transport Layer Security (TLS) adalah protokol keamanan yang digunakan untuk melindungi proses komunikasi data antara client dan server melalui jaringan internet. TLS berfungsi untuk mengenkripsi data yang sedang dikirim sehingga informasi tersebut tidak dapat dibaca atau dimodifikasi oleh pihak lain selama proses transmisi.

TLS merupakan pengembangan dari Secure Sockets Layer (SSL) yang saat ini sudah tidak lagi digunakan karena memiliki beberapa kelemahan keamanan.

Pada implementasinya, TLS bekerja dengan melakukan proses pertukaran kunci (handshake) sebelum komunikasi berlangsung. Setelah proses tersebut selesai, seluruh data yang dikirim akan dienkripsi sehingga hanya client dan server yang dapat membacanya.

Dalam penelitian ini, TLS digunakan melalui protokol HTTPS untuk mengamankan komunikasi antara pengguna dengan website Gals Collection. Dengan demikian, data login, checkout, dan informasi lainnya tetap terlindungi selama proses transmisi.

### *2.1.9 HTTP /HTTPS*

Hypertext Transfer Protocol (HTTP) merupakan protokol komunikasi yang digunakan untuk mengirimkan data antara web browser dan web server. HTTP memungkinkan pengguna mengakses halaman website melalui internet. Namun, HTTP tidak memiliki mekanisme enkripsi sehingga seluruh data yang dikirim dapat dibaca apabila berhasil disadap oleh pihak lain.

Hypertext Transfer Protocol Secure (HTTPS) merupakan pengembangan dari HTTP yang menggunakan protokol TLS untuk mengenkripsi komunikasi data. Dengan adanya TLS, informasi yang dikirimkan antara client dan server akan terlindungi sehingga tidak dapat dibaca oleh pihak yang tidak berwenang.

Pada penelitian ini, website Gals Collection menggunakan HTTPS sehingga proses login, checkout, dan transaksi pengguna dilakukan melalui jalur komunikasi yang aman. Penggunaan HTTPS menjadi salah satu lapisan keamanan yang melindungi data selama proses transmisi (data in transit), sedangkan algoritma AES-128 digunakan untuk melindungi data yang telah tersimpan di dalam database (data at rest).

### *2.1.10 SQL Injection*

SQL Injection merupakan salah satu jenis serangan pada aplikasi web yang memanfaatkan kelemahan dalam proses pengolahan input pengguna. Serangan ini dilakukan dengan menyisipkan perintah SQL berbahaya ke dalam input aplikasi sehingga penyerang dapat memanipulasi query yang dijalankan oleh database.

Apabila aplikasi tidak memiliki mekanisme keamanan yang baik, SQL Injection dapat digunakan untuk membaca, mengubah, menghapus, bahkan

mengambil seluruh isi database. Oleh karena itu, SQL Injection menjadi salah satu ancaman keamanan yang paling sering ditemukan pada aplikasi berbasis web.

Salah satu cara untuk mencegah SQL Injection adalah menggunakan Prepared Statement atau Parameterized Query, yaitu memisahkan perintah SQL dengan data yang dimasukkan oleh pengguna. Dengan cara ini, input pengguna akan diperlakukan sebagai data sehingga tidak dapat dijalankan sebagai perintah SQL.

Pada penelitian ini dilakukan pengujian menggunakan SQLMap untuk mengetahui apakah website Gals Collection masih memiliki kerentanan terhadap serangan SQL Injection setelah sistem selesai dikembangkan.

### *2.1.11 SQLMap*

SQLMap merupakan perangkat lunak open source yang digunakan untuk mendeteksi dan menguji kerentanan SQL Injection secara otomatis pada aplikasi web. SQLMap mampu melakukan berbagai teknik pengujian, seperti Boolean-Based Blind, Error-Based, Time-Based Blind, dan UNION Query, untuk mengetahui apakah suatu parameter dapat dieksploitasi menjadi serangan SQL Injection.

Selain mendeteksi kerentanan, SQLMap juga dapat digunakan untuk memperoleh informasi mengenai database, seperti nama database, daftar tabel, struktur tabel, hingga isi data apabila aplikasi benar-benar rentan terhadap SQL Injection.

Dalam penelitian ini, SQLMap digunakan sebagai alat pengujian keamanan untuk mengevaluasi ketahanan website Gals Collection terhadap serangan SQL Injection. Hasil pengujian menunjukkan bahwa SQLMap tidak berhasil menemukan celah SQL Injection pada parameter yang diuji sehingga website memiliki ketahanan terhadap jenis serangan tersebut.

### *2.1.12 Framework Pengembangan Sistem E-Commerce*

Dalam pengembangan sistem *e-commerce*, terdapat beberapa framework dan teknologi yang dapat digunakan, antara lain:

1) Laravel: Framework PHP yang populer untuk pengembangan aplikasi web dengan fitur keamanan bawaan yang kuat.

2) CodeIgniter: Framework PHP ringan dan cepat dengan arsitektur MVC yang mendukung pengembangan aplikasi *e-commerce*.
3) React/Vue.js: Library JavaScript untuk membangun antarmuka pengguna yang interaktif, sering digunakan dengan backend berbasis API.
4) MySQL/PostgreSQL: Sistem manajemen basis data relasional yang umum digunakan dalam aplikasi *e-commerce*.
5) RESTful API: Arsitektur untuk membangun layanan web yang mendukung komunikasi antar sistem.

Framework dan teknologi yang dipilih harus mendukung implementasi enkripsi AES dengan efisien dan aman. Pemilihan framework dan teknologi yang tepat dapat mempengaruhi tingkat keamanan dan performa sistem *e-commerce* secara keseluruhan.

Dalam pengembangan sistem *e-commerce* untuk Toko Gals Collection, akan menggunakan kombinasi framework dan teknologi yang mendukung implementasi enkripsi AES seperti:

1) PHP Native (tanpa framework besar seperti Laravel, CodeIgniter, Symfony).
2) phpMyAdmin untuk database.
3) HTML, CSS, dan JavaScript standar untuk antarmuka pengguna.

Dengan mempertimbangkan keseimbangan antara keamanan dan kemudahan penggunaan.

## 2.2 Penelitian Terdahulu

Pada bagian ini, akan dipaparkan beberapa penelitian terdahulu yang berkaitan dengan topik penelitian ini. Hal ini bertujuan agar dapat dilakukan perbandingan antara penelitian ini dengan penelitian sebelumnya, serta pengambilan referensi yang mendukung penyusunan penelitian ini. Beberapa penelitian terdahulu tersebut adalah sebagai berikut:

Muttaqin (2024), dalam penelitiannya yang berjudul "Implementasi Algoritma *Advanced Encryption Standard* (AES) untuk Keamanan Transaksi *e-commerce*", menunjukkan bahwa penggunaan AES-128 mampu meningkatkan keamanan data transaksi dengan tingkat perlindungan yang signifikan. Studi tersebut menemukan bahwa proses enkripsi dan dekripsi menggunakan AES-128 berlangsung cukup efisien, tanpa mengganggu performa sistem secara keseluruhan.

Rata-rata waktu yang dibutuhkan untuk mengenkripsi data sebesar 1 MB adalah 0,0045 detik.

Mustika (2020), melalui penelitian berjudul "Penerapan Enkripsi AES pada Sistem Login dan Penyimpanan Data Pengguna *e-commerce*", membuktikan bahwa implementasi algoritma AES dapat mengurangi risiko kebocoran informasi hingga 67% dibandingkan sistem tanpa enkripsi. Selain itu, penelitian ini juga menunjukkan bahwa AES dapat diintegrasikan ke dalam sistem login tanpa mempengaruhi kecepatan akses pengguna secara signifikan.

Abdul Hussien dkk. (2021) dalam penelitian berjudul "A Secure Environment Using a New Lightweight AES Encryption Algorithm for *e-commerce* Websites", mengusulkan algoritma AES ringan dengan modifikasi seperti pengurangan ronde dan penggunaan teknik padding serta zigzag. Penelitian ini bertujuan untuk meningkatkan efisiensi enkripsi tanpa mengurangi tingkat keamanan dalam lingkungan *e-commerce*. Hasilnya menunjukkan bahwa algoritma ini dapat mengenkripsi data 2,8 detik lebih cepat dari AES standar, dengan konsumsi CPU yang lebih rendah dan efek avalanche yang lebih baik sebesar 14,3%. Meskipun demikian, penting dicatat bahwa artikel ini telah ditarik kembali (retracted) oleh jurnal karena masalah integritas publikasi.

Ifani dkk. (2025)melalui jurnal berjudul "Application of *Advanced Encryption Standard* (AES) Algorithm in *e-commerce* Login System for User Data Security", meneliti penerapan algoritma AES pada sistem login *e-commerce* untuk mencegah serangan siber seperti trapdoor attack. Penelitian dilakukan dengan pengujian sebelum dan sesudah penerapan AES menggunakan alat seperti Burp Suite. Hasilnya menunjukkan bahwa username dan password pengguna berhasil dienkripsi menjadi ciphertext dan tidak dapat lagi dilihat oleh pihak ketiga yang tidak berwenang, sehingga sistem lebih aman dari penyadapan.

Simarmata dkk. (2018) dalam penelitian "Implementation of AES Algorithm for Information Security of Web-Based Application", menerapkan algoritma AES untuk mengenkripsi dan mendekripsi file teks dan gambar pada aplikasi web. Penelitian ini mendemonstrasikan penggunaan berbagai panjang kunci AES (128, 192, dan 256 bit) dengan mode ECB dan CBC. Hasilnya menunjukkan bahwa aplikasi dapat berjalan dengan baik, menjaga kerahasiaan informasi, serta

memastikan bahwa isi file tidak berubah setelah proses dekripsi, menjadikan AES sebagai metode yang efektif untuk menjaga keamanan data berbasis web.

Penelitian ini (2025), berjudul "Pengembangan Sistem Informasi *e-commerce* dengan Enkripsi AES untuk Keamanan Transaksi Toko Gals Collection", bertujuan untuk merancang dan mengembangkan sistem *e-commerce* yang mengedepankan keamanan data pengguna dan transaksi. Penelitian ini mengimplementasikan enkripsi AES-128 guna meningkatkan perlindungan terhadap data sensitif tanpa mengorbankan performa maupun kenyamanan pengguna. Sistem dirancang agar mampu menjaga kerahasiaan informasi akun dan transaksi, menjadikannya lebih tahan terhadap potensi ancaman keamanan siber dalam lingkungan *e-commerce*.

Dibandingkan dengan penelitian-penelitian terdahulu yang hanya berfokus pada aspek enkripsi untuk login atau transaksi secara terpisah, penelitian ini merancang dan mengembangkan sistem informasi *e-commerce* secara menyeluruh dengan penerapan algoritma *Advanced Encryption Standard* (AES-128) untuk melindungi baik data transaksi maupun data akun pengguna. Sistem ini dirancang untuk tidak hanya meningkatkan keamanan. Dengan pendekatan ini, penelitian ini menghadirkan solusi yang lebih utuh dalam hal perlindungan data dan kepercayaan pengguna terhadap sistem *e-commerce*, khususnya pada toko Gals Collection.

Tabel 2.1 Perbandingan variabel penelitian

| **Kategori** | **Peneliti 1** | **Peneliti 2** | **Peneliti 3** | **Peneliti 4** | **Peneliti 5** | **Peneliti 6** |
|---|---|---|---|---|---|---|
| Penelitian | Muttaqin & Indonesia (2024) | Mustika (2020) | Abdul Hussien et al. (2021) | Ifani et al. (2025) | (Simarmata et al., 2018) | Penelitian ini (2025) |
| Metode | Enkripsi AES-128 | Enkripsi AES | Lightweight AES | Enkripsi AES-128 | Enkripsi AES (128,192, 256) | Enkripsi AES-128 |
| Pengujian | Pengujian proses enkripsi dan dekripsi | Pengujian login dan data customer | Pengujian kecepatan enkripsi CPU, dan avalance effect | Pengujian login menggunakan Burpsuite | Pengujian enkripsi dan dekripsi file teks dan gambar | Pengujian keamanan transaksi dan akun pengguna |
| Data | Data transaksi *e-commerce* | Data login dan data customer | Data transaksi *e-commerce* | Username dan Password pengguna | File teks dan gambar | Data transaksi dan akun pengguna |

| Kategori | Peneliti 1 | Peneliti 2 | Peneliti 3 | Peneliti 4 | Peneliti 5 | Peneliti 6 |
|---|---|---|---|---|---|---|
| | | | | | | *e-commerce* |
| Fokus Penelitian | Keamanan transaksi, integritas data, dan performa sistem | Keamanan login dan perlindungan data customer | Kecepatan enkripsi, penggunaan CPU, dan avalanche effect | Keamanan login, enkripsi username/ password, dan pencegahan penyadapan | Keamanan file serta proses enkripsi dan dekripsi | Keamanan transaksi, perlindungan data pengguna, dan ketahanan terhadap kebocoran database |
| Hasil | AES-128 menungkatkan kemaanan transaksi tanpa menggangu peforma | AES meningkatkan keamanan login dan data customer | Lightweight AES lebih cepat dan efisien dibanding AES standar | Data login berhasil dienkripsi menjadi chipertext | AES berhasil mengenkripsi dan mendekrisi file tanpa mengubah isi file. | AES-128 dirancang meningkatkan keamanan transaksi dan akun pengguna |

Berdasarkan kajian terhadap beberapa penelitian terdahulu pada Tabel 2.1 (Politeknik Caltex Riau, 2026), diketahui bahwa penelitian-penelitian tersebut telah membahas penerapan algoritma *Advanced Encryption Standard* (AES) pada sistem *e-commerce*, terutama pada keamanan trnasaksi, login, dan perlindungan data pengguna. Namun, penelitian-penelitian tersebut masih memiliki keterbatasan, seperti hanya berfokus pada keamanan login, kemanaan transaksi secara terpisah, maupun pengujian peforma algoritma enkripsi tanpa mengintegritaskan keamanan sistem *e-commerce* secara menyeluruh.

Penelitian ini memiliki perbedaan dengan penelitian sebelumnya karena penelitian ini merancang dan mengembangkan sistem informasi *e-commerce* degan penerapan algoritma AES-128 untuk melindungi data transaksi serta akun pengguna secara terpadu pada toko Gals Collection. Selain menitikberatkan pada keamanan data, penelitian ini juga memperhatikan peforma sistem dan kenyamanan pengguna dalam melakukan transaksi online. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi dalam meningkatkan keamanan sistem *e-commerce* seta melengkapi hsil-hasil penelitian sebelumnya terkait implementasi algoritma AES yang telah ada sebelumnya.