

BAB 2

TINJAUAN PUSTAKA

2.1 Landasan Teori

Berikut merupakan landasan teori terkait perancangan dan pengembangan sistem e-commerce yang digunakan sebagai dasar acuan dalam penelitian ini. Teori-teori yang dipaparkan mencakup berbagai konsep dan definisi yang berkaitan langsung dengan sistem yang akan dibangun, sehingga dapat memberikan pemahaman yang lebih mendalam mengenai topik yang dibahas. Pemaparan landasan teori ini diharapkan dapat menjadi pedoman yang kuat dalam proses analisis, perancangan, serta implementasi sistem secara keseluruhan.

2.1.1 E-Commerce

E-Commerce (Electronic Commerce) merupakan aktivitas jual beli barang dan jasa yang dilakukan secara elektronik melalui jaringan internet. Menurut Laudon & Traver (2019), e-commerce adalah penggunaan internet dan web untuk melakukan transaksi bisnis. Lebih lanjut, e-commerce mencakup seluruh proses transaksi mulai dari pencarian informasi produk, pemesanan, pembayaran, hingga pengiriman barang yang semuanya dilakukan secara digital.

E-commerce memiliki beberapa jenis model bisnis, di antaranya *Business-to-Consumer* (B2C) yaitu transaksi antara pelaku usaha dengan konsumen akhir, *Business-to-Business* (B2B) yaitu transaksi antar pelaku usaha, serta *Consumer-to-Consumer* (C2C) yaitu transaksi antar sesama konsumen melalui platform perantara. Dalam konteks penelitian ini, aplikasi penjualan karya digital yang dikembangkan termasuk dalam kategori C2C dan B2C, di mana kreator digital menjual karyanya langsung kepada konsumen melalui platform yang disediakan.

Keunggulan utama *e-commerce* meliputi kemudahan akses tanpa batas geografis, efisiensi waktu dan biaya operasional, serta kemampuan untuk menjangkau pasar yang lebih luas dibandingkan toko konvensional. Namun, e-commerce juga menghadapi berbagai tantangan, terutama terkait keamanan data pengguna dan kepercayaan konsumen dalam melakukan transaksi secara online (Turban et al., 2018).

2.1.2 Keamanan Transaksi E-Commerce

Keamanan transaksi e-commerce merupakan aspek fundamental yang harus diperhatikan dalam setiap sistem perdagangan elektronik. Keamanan dalam konteks ini mencakup perlindungan terhadap data pribadi pengguna, integritas informasi transaksi, kerahasiaan data keuangan, serta ketersediaan layanan sistem. Menurut Stallings (2017), terdapat tiga prinsip utama keamanan informasi yang sering disebut sebagai *CIA Triad*, yaitu *Confidentiality* (kerahasiaan), *Integrity* (integritas), dan *Availability* (ketersediaan).

Ancaman keamanan yang umum terjadi pada sistem e-commerce antara lain phishing, pencurian identitas (*identity theft*), serangan *man-in-the-middle*, serta peretasan akun pengguna. Phishing merupakan teknik penipuan yang dilakukan dengan cara menyamar sebagai entitas terpercaya untuk mencuri informasi sensitif pengguna, seperti kata sandi dan data kartu kredit. Serangan-serangan tersebut dapat menyebabkan kerugian finansial dan hilangnya kepercayaan pengguna terhadap platform *e-commerce* (Putra et al., 2024).

Untuk mengatasi berbagai ancaman tersebut, diperlukan penerapan mekanisme keamanan yang berlapis pada sistem e-commerce. Beberapa mekanisme yang umum digunakan antara lain enkripsi data menggunakan algoritma seperti AES (*Advanced Encryption Standard*) atau SSL/TLS, penggunaan protokol HTTPS untuk komunikasi yang aman, serta penerapan sistem autentikasi berlapis seperti *Two-Factor Authentication* (2FA). Kombinasi berbagai mekanisme keamanan ini bertujuan untuk menciptakan sistem yang dapat melindungi pengguna dari berbagai ancaman siber sekaligus mempertahankan kenyamanan dalam bertransaksi.

2.1.3 Two-Factor Authentication

Two-Factor Authentication (2FA) adalah metode autentikasi keamanan yang mengharuskan pengguna untuk memverifikasi identitasnya melalui dua tahap yang berbeda sebelum dapat mengakses sebuah sistem atau akun. Metode ini didasarkan pada kombinasi dua dari tiga faktor autentikasi, yaitu sesuatu yang diketahui pengguna (*something you know*) seperti kata sandi, sesuatu yang dimiliki pengguna (*something you have*) seperti perangkat mobile atau token, dan

sesuatu yang melekat pada pengguna (something you are) seperti sidik jari atau pengenalan wajah (NIST, 2017).

Salah satu implementasi 2FA yang paling umum digunakan adalah pengiriman kode OTP (*One-Time Password*) melalui email atau SMS. OTP merupakan kode verifikasi yang hanya berlaku satu kali dan memiliki masa berlaku terbatas, biasanya antara 5 hingga 10 menit. Cara kerja 2FA dengan OTP adalah sebagai berikut: pertama, pengguna memasukkan nama pengguna dan kata sandi; kedua, sistem mengirimkan kode OTP ke email atau nomor telepon pengguna yang telah terdaftar; ketiga, pengguna memasukkan kode OTP tersebut untuk menyelesaikan proses login. Dengan mekanisme ini, meskipun kata sandi pengguna berhasil dicuri, pelaku kejahatan tetap tidak dapat mengakses akun tanpa kode OTP yang dikirim ke perangkat pribadi pengguna (Hapsari et al., 2020).

Penerapan 2FA telah terbukti secara signifikan meningkatkan keamanan akun pengguna. Berdasarkan penelitian Putra et al. (2024), implementasi 2FA mampu mengurangi risiko peretasan akun hingga 99,9% dibandingkan dengan penggunaan kata sandi tunggal. Dalam konteks aplikasi penjualan karya digital, penerapan 2FA memberikan lapisan perlindungan tambahan yang sangat penting, terutama untuk melindungi data transaksi dan karya digital milik pengguna dari akses tidak sah.

2.1.4 Framework Pengembangan Sistem E-Commerce

Framework merupakan kerangka kerja atau struktur dasar yang digunakan sebagai fondasi dalam pengembangan perangkat lunak. Penggunaan framework dalam pengembangan sistem e-commerce bertujuan untuk mempercepat proses pengembangan, meningkatkan kualitas kode, serta memastikan konsistensi dan keamanan sistem. Framework menyediakan berbagai komponen yang telah teruji, termasuk fitur keamanan bawaan, manajemen sesi, dan perlindungan terhadap serangan umum seperti SQL Injection dan Cross-Site Scripting (XSS).

Dalam pengembangan aplikasi penjualan karya digital ini, digunakan framework berbasis web yang mendukung arsitektur Model-View-Controller (MVC). Arsitektur MVC memisahkan logika bisnis (Model), tampilan antarmuka

(View), dan pengendali alur aplikasi (Controller), sehingga kode menjadi lebih terstruktur, mudah dipelihara, dan dikembangkan lebih lanjut. Laravel merupakan salah satu framework PHP yang banyak digunakan dalam pengembangan sistem e-commerce karena menyediakan fitur autentikasi yang lengkap, sistem routing yang fleksibel, serta dukungan terhadap berbagai mekanisme keamanan.

Selain framework back-end, pengembangan sistem e-commerce juga memanfaatkan framework front-end untuk membangun antarmuka pengguna yang responsif dan interaktif. Framework seperti Bootstrap atau Tailwind CSS digunakan untuk memastikan tampilan aplikasi dapat menyesuaikan diri dengan berbagai ukuran layar perangkat, baik desktop maupun mobile. Kombinasi framework back-end dan front-end ini memungkinkan pengembangan aplikasi yang efisien sekaligus menghasilkan produk yang berkualitas tinggi dari sisi fungsionalitas dan pengalaman pengguna

2.1.5 Database

Database atau basis data adalah kumpulan data yang terorganisir secara sistematis dan dapat diakses, dikelola, serta diperbarui secara efisien. Dalam konteks sistem e-commerce, database berfungsi sebagai tempat penyimpanan seluruh data yang diperlukan oleh sistem, meliputi data pengguna, informasi produk, riwayat transaksi, serta data keamanan seperti token autentikasi. Sistem Manajemen Basis Data (DBMS) yang banyak digunakan dalam pengembangan aplikasi web adalah MySQL dan PostgreSQL karena keduanya bersifat open-source, memiliki performa yang baik, serta mendukung fitur keamanan yang memadai (Ramakrishnan & Gehrke, 2003).

Dalam pengembangan aplikasi penjualan karya digital ini, perancangan database dilakukan dengan mempertimbangkan kebutuhan fungsional sistem serta aspek keamanan data. Normalisasi database dilakukan untuk menghilangkan redundansi data dan memastikan integritas referensial antar tabel. Selain itu, data sensitif seperti kata sandi pengguna disimpan dalam bentuk terenkripsi menggunakan algoritma hashing, sehingga meskipun database berhasil diakses secara tidak sah, data sensitif tersebut tidak dapat dibaca secara langsung.

Pengelolaan database dalam sistem e-commerce juga mencakup penanganan transaksi (transaction handling) untuk memastikan konsistensi data. Mekanisme ACID (Atomicity, Consistency, Isolation, Durability) yang didukung oleh MySQL dan PostgreSQL menjamin bahwa setiap transaksi data berjalan secara utuh dan konsisten, bahkan dalam kondisi kegagalan sistem sekalipun. Hal ini sangat penting dalam sistem penjualan karya digital untuk memastikan bahwa setiap transaksi pembelian tercatat dengan benar dan tidak terjadi inkonsistensi data.

2.1.6 Visual Code Studio

E-Commerce Visual Studio Code (VS Code) adalah editor kode sumber (source code editor) yang dikembangkan oleh Microsoft dan dirilis secara gratis sebagai perangkat lunak open-source. VS Code mendukung berbagai bahasa pemrograman dan memiliki ekosistem ekstensi yang sangat kaya, sehingga dapat dikustomisasi sesuai kebutuhan pengembangan. Fitur-fitur utama VS Code meliputi syntax highlighting, IntelliSense (penyelesaian kode otomatis), debugging terintegrasi, kontrol versi melalui Git, serta terminal terintegrasi yang memudahkan proses pengembangan aplikasi (Microsoft, 2023).

Dalam pengembangan aplikasi penjualan karya digital ini, Visual Studio Code digunakan sebagai editor utama karena kemudahannya dalam mendukung pengembangan aplikasi web secara menyeluruh. Berbagai ekstensi yang tersedia pada VS Code, seperti PHP Intelephense untuk pengembangan PHP, Prettier untuk pemformatan kode, serta ekstensi database client untuk manajemen basis data, sangat membantu dalam meningkatkan produktivitas pengembang. Selain itu, fitur Live Share pada VS Code memungkinkan kolaborasi pengembangan secara real-time yang memudahkan koordinasi antar anggota tim.

VS Code juga terintegrasi dengan baik dengan sistem kontrol versi Git, sehingga pengelolaan kode sumber dapat dilakukan secara efisien langsung dari dalam editor. Fitur diff viewer dan branch management yang tersedia memudahkan pengembang dalam melacak perubahan kode, mengelola versi aplikasi, serta berkolaborasi dalam pengembangan proyek. Popularitas VS Code

yang sangat tinggi di kalangan pengembang web menjadikannya pilihan yang tepat sebagai lingkungan pengembangan utama dalam penelitian ini.

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:

1. Putra (2024), dalam penelitiannya yang berjudul "*Analysis of Phishing Attack Trends, Impacts and Prevention Methods: Literature Study*", menunjukkan bahwa serangan phishing terus berkembang dengan teknik yang semakin kompleks seperti spear phishing, whaling, dan smishing. Penelitian ini menemukan bahwa metode pencegahan seperti filter email, enkripsi, serta penerapan *Two-Factor Authentication* (2FA) mampu meningkatkan keamanan sistem secara signifikan. Selain itu, kesadaran pengguna menjadi faktor penting dalam mengurangi keberhasilan serangan phishing.
2. Radiansyah & Priyadi (2016), melalui penelitian berjudul "*Analisis Faktor Penyebab dan Pencegahan Phishing Menggunakan Systematic Literature Review*", menjelaskan bahwa rendahnya pengetahuan pengguna menjadi salah satu penyebab utama keberhasilan serangan phishing. Penelitian ini menunjukkan bahwa pencegahan dapat dilakukan melalui edukasi pengguna serta penerapan sistem keamanan tambahan seperti autentikasi berlapis.
3. Wijoyo (tahun tidak disebutkan), dalam penelitiannya tentang analisis jenis dan pencegahan phishing, membahas berbagai bentuk serangan phishing seperti email phishing, web phishing, dan smishing. Hasil penelitian menunjukkan bahwa seluruh jenis serangan tersebut bertujuan untuk memperoleh data sensitif pengguna, sehingga diperlukan sistem keamanan yang lebih kuat untuk melindungi informasi tersebut..
4. Danuri (tahun tidak disebutkan), dalam penelitian berjudul "*Perkembangan Teknologi Informasi dan Dampaknya terhadap Kejahatan Siber*", menjelaskan

bahwa pesatnya perkembangan teknologi informasi juga meningkatkan risiko kejahatan siber, termasuk phishing. Penelitian ini menekankan pentingnya penerapan sistem keamanan yang lebih baik serta regulasi untuk melindungi data pengguna dalam lingkungan digital.

5. Penelitian oleh Yani (2016) juga menyoroti pentingnya penerapan sistem keamanan tambahan dalam mencegah serangan siber. Hasil penelitian menunjukkan bahwa penggunaan teknologi seperti Two-Factor Authentication (2FA), enkripsi, serta edukasi pengguna dapat menjadi solusi efektif dalam meningkatkan keamanan sistem informasi
6. Penelitian ini (2026), berjudul *"Perancangan Aplikasi Penjualan Karya Digital dengan Sistem Keamanan Two-Factor Authentication"*, bertujuan untuk merancang dan mengembangkan aplikasi penjualan karya digital berbasis web yang mengedepankan keamanan akun pengguna. Penelitian ini mengimplementasikan sistem Two-Factor Authentication (2FA) menggunakan metode verifikasi kode OTP untuk memberikan lapisan keamanan tambahan. Sistem dirancang agar mampu melindungi akun pengguna dari akses tidak sah tanpa mengurangi kenyamanan dan efisiensi dalam proses transaksi digital.

Dibandingkan dengan penelitian-penelitian terdahulu yang lebih banyak berfokus pada pencegahan *phishing* atau keamanan sistem secara umum, penelitian ini merancang dan mengembangkan aplikasi penjualan karya digital secara menyeluruh dengan penerapan sistem autentikasi ganda (2FA). Sistem ini tidak hanya meningkatkan keamanan akun pengguna, tetapi juga tetap mempertahankan kemudahan penggunaan dan efisiensi transaksi. Dengan pendekatan ini, penelitian ini memberikan solusi yang lebih terintegrasi dalam menjaga keamanan serta meningkatkan kepercayaan pengguna terhadap platform e-commerce.

Tabel.1 Perbandingan variabel penelitian

Kategori	Peneliti 1	Peneliti 2	Peneliti 3
Metode	Studi literatur / literature review	Systematic Literature Review (SLR)	Kajian pustaka dan analisis penerapan teknologi keamanan
Pengujian	Analisis teoritis	Analisis teoritis	Kajian teoritis

Kategori	Peneliti 1	Peneliti 2	Peneliti 3
	terhadap penelitian sebelumnya	berdasarkan literatur ilmiah	tidak ada implementasi langsung
Sumber Data	Literatur dan jurnal terkait trend phishing.	Literatur ilmiah terkait phishing dan fator penyebabnya.	Referensi dan literatur keamanan sistem informasi
Fokus keamanan	Pencegahan phishing melalui filter email, enkripsi, dan 2FA	Edukasi pengguna dan autentikasi berlapis sebagai pencegahan phishing	Penerapan 2FA, enkripsi, dan edukasi pengguna untuk keamanan sistem
Teknologi yang di usulkan	Two-Factor Authentication (2FA), enkripsi, filter email	Autentikasi berlapis, sistem edukasi keamanan pengguna	Two-Factor Authentication (2FA), enkripsi data
Hasil / kesimpulan	2FA dan enkripsi mampu meningkatkan keamanan sistem secara signifikan	Edukasi pengguna dan keamanan berlapis efektif mengurangi serangan phishing	Kombinasi 2FA dan enkripsi menjadi solusi efektif keamanan sistem informasi

Berdasarkan kajian terhadap beberapa penelitian terdahulu pada Tabel 2.1 (Politeknik Caltex Riau, 2026), diketahui bahwa penelitian-penelitian tersebut telah membahas topik yang relevan dengan penelitian ini, namun memiliki keterbatasan dari sisi implementasi Two-Factor Authentication (2FA) yang masih bersifat teoritis tanpa penerapan langsung pada sistem, cakupan pembahasan yang belum mencakup integrasi keamanan pada platform transaksi digital, maupun aspek pengujian empiris terhadap efektivitas 2FA dalam melindungi akun pengguna secara nyata.

Penelitian ini memiliki perbedaan dengan penelitian sebelumnya karena mengkaji permasalahan keamanan akun pada aplikasi penjualan karya digital berbasis web dengan mengimplementasikan sistem Two-Factor Authentication (2FA) berbasis OTP secara langsung dan menyeluruh, dengan menyesuaikan pendekatan penelitian terhadap kebutuhan dan karakteristik objek penelitian. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi pada pengembangan aplikasi penjualan digital yang aman, praktis, dan terlindungi dari