1. PENDAHULUAN

1.1. Latar Belakang

Seiring meningkatnya insiden serangan siber dalam pelayanan publik digital, keamanan data dan privasi masyarakat saat ini menjadi isu yang sangat krusial. Laporan dari Badan Siber dan Sandi Negara (BSSN) tahun 2024 menunjukkan bahwa sektor publik, yaitu sistem pemerintahan menjadi yang paling terdampak oleh adanya insiden keamanan siber, tercatat sejumlah 183 dugaan insiden kebocoran data, bahkan lebih dari 32 juta data terekspos di situs darknet. Jumlah ini merupakan jumlah paling tinggi dibanding sektor lainnya di Indonesia. Selain itu, ditemukan sejumlah 4.071 kasus *web defacement* pada situs pemerintahan [1]. Kondisi ini sangat memprihatinkan, karena tidak hanya mengancam keamanan data masyarakat, melainkan juga dapat merusak kepercayaan publik terhadap pemerintah dan mengganggu kelancaran pelayanan yang mengandalkan sistem digital.

Tingginya angka insiden serangan siber tersebut mengindikasikan adanya kelemahan dalam sistem pemerintahan. Salah satu lemahnya suatu sistem disebabkan karena tidak mengintegrasikan aspek keamanan sejak tahap awal pengembangan [2]. Banyak sistem layanan publik digital yang masih mengandalkan pendekatan pengembangan tradisional seperti *Software Development Life Cycle* (SDLC), yang seringkali baru dipertimbangkan pada tahap akhir pengembangan [3]. Hal ini mengakibatkan banyaknya potensi celah keamanan yang tidak terdeteksi sejak dini, sehingga meningkatkan risiko terhadap kerahasiaan, integritas, dan ketersediaan sistem layanan publik digital [4].

Untuk mengatasi permasalahan tersebut, pendekatan *Secure* SDLC dapat diterapkan dengan mengintegrasikan prinsip keamanan dalam setiap fase pengembangan sistem [5]. *Secure* SDLC menekankan pada identifikasi dan mitigasi risiko keamanan sejak tahap awal secara lebih proaktif [6]. Pendekatan ini juga memungkinkan untuk meminimalisasikan kemungkinan

terjadinya potensi celah keamanan dan meningkatkan ketahanan sistem terhadap serangan [7]

Meskipun *Secure* SDLC memberikan pendekatan yang lebih proaktif, penerapannya tidak lepas dari berbagai tantangan. Proses ini memerlukan alokasi sumber daya yang lebih besar, yang seringkali menjadi kendala dalam proyek pengembangan perangkat lunak [8]. Selain itu, integrasi aspek keamanan pada tiap tahapan menambah tingkat kompleksitas, sehingga perlu perencanaan yang matang, pengelolaan dan pengawasan yang lebih ekstra [9]. Oleh karena itu, diperlukannya pendekatan alternatif yang dapat mendukung dan membantu penerapan *Secure* SDLC secara lebih adaptif.

Seiring dengan kemajuan teknologi, pemanfaatan kecerdasan buatan dalam pengembangan perangkat lunak semakin menunjukkan perhatian, terutama dalam upaya meningkatkan kualitas dan keamanan sistem [10]. Salah satunya adalah Generative AI yang telah mulai digunakan dalam berbagai fase SDLC, untuk membantu pengembangan sistem yang lebih adaptif terhadap kebutuhan teknis dan risiko keamanan [11]. Studi oleh Zakkiya. menunjukkan bahwa *generative* AI, khususnya melalui pemanfaatan ChatGPT-4o, dapat mendukung proses pengembangan perangkat lunak yang aman dengan meningkatkan kelengkapan dan keselarasan dokumentasi terhadap standar keamanan [5]. Selain itu, teknologi Generative AI dinilai mampu menyederhanakan prinsip-prinsip keamanan secara otomatis yang sebelumnya memerlukan proses manual yang kompleks [12].

Kebutuhan ini semakin relevan untuk diterapkan pada tingkat pemerintahan di pedesaan yang masih menghadapi tantangan dalam digitalisasi layanan publik. Salah satunya adalah Desa Limapoccoe, yang hingga saat ini masih mengandalkan proses manual dalam penyelenggaraan layanan publik, khususnya dalam pengelolaan administrasi, persebaran informasi, pengelolaan data, hingga penanganan pengaduan. Kondisi ini menyulitkan masyarakat untuk mengakses layanan publik yang cepat hingga keterlambatan dalam proses pelayanan. Selain itu, belum adanya sistem yang

terdigitalisasi juga menimbulkan tantangan bagi pemerintah terutama perihal pendokumentasian dan pelaporan data masyarakat desa yang tidak aman dan kurang terstruktur.

Berdasarkan permasalahan tersebut, eksplorasi lebih lanjut terhadap pendekatan pengembangan sistem yang mendukung integrasi aspek keamanan sejak tahap awal diperlukan, seperti *Secure* SDLC dalam konteks pengembangan sistem layanan publik di tingkat Desa dengan bantuan *Generative* AI terutama untuk proses dokumentasi dan menghasilkan kode aman. Oleh karena itu, penelitian ini difokuskan pada pemanfaatan *Generative* AI untuk mendukung penerapan *Secure* SDLC dalam pengembangan sistem layanan publik di tingkat desa berbasis digital dengan mengintegrasikan aspek keamanan, terutama pada sisi backend yang memiliki peran penting dalam pengelolaan data, proses layanan, dan kontrol keamanan.

1.2. Rumusan Masalah

Berdasarkan latar belakang masalah tersebut, adapun rumusan masalah yang akan dicapai dalam penelitian ini adalah sebagai berikut.

1. Bagaimana Secure SDLC berbasis *Generative* AI dapat diterapkan pada pengembangan *backend* sistem layanan publik Desa Limapoccoe?
2. Bagaimana fase *security development* pada *Secure* SDLC berbasis Generative AI dapat diadopsi dalam pengembangan *backend* sistem layanan publik Desa Limapoccoe?
3. Bagaimana hasil adopsi fase *security development* pada Secure SDLC berbasis *Generative* AI dapat dianalisis dan dievaluasi dalam pengembangan backend sistem layanan publik Desa Limapoccoe?

1.3. Tujuan dan Manfaat

Penelitian ini bertujuan untuk mengeksplorasi proses adopsi *Secure* SDLC berbasis *Generative* AI dalam pengembangan *backend* sistem layanan publik Desa Limapoccoe, yang berfokus pada fase *security development*

untuk meninjau bagaimana Generative AI, khususnya ChatGPT 4o, dapat dimanfaatkan sebagai alat bantu dalam menerapkan aspek keamanan fase tersebut.

Manfaat dari penelitian ini diharapkan dapat dirasakan oleh berbagai pihak. Bagi pengembang, penelitian ini dapat memberikan wawasan tentang penggunaan Generative AI untuk pengembangan *backend* yang aman. Bagi pemerintah desa, hasilnya dapat digunakan sebagai contoh dalam membangun layanan publik digital yang aman. Terakhir, bagi akademisi, penelitian ini dapat memperkaya kajian mengenai integrasi Generative AI dalam Secure SDLC terutama dalam konteks layanan publik digital desa.

1.4. Batasan Masalah

Penelitian ini memiliki beberapa batasan yang ditetapkan untuk menyederhanakan ruang lingkup permasalahan agar dapat diselesaikan dalam waktu yang tersedia.

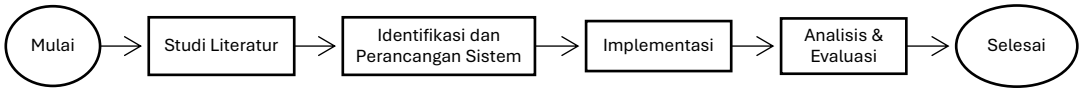
1. Penelitian ini melakukan eksplorasi yang merujuk pada panduan *Secure* SDLC berbasis Generative AI, berjudul "*A Guideline for the Adoption of Generative AI to Support Secure Software Development Life Cycle (SSDLC): A Case Study of ChatGPT*". Panduan ini digunakan sebagai kerangka awal untuk menerapkan keamanan dan integrasi Generative AI berbasis *prompting*. Penelitian ini secara khusus melakukan eksplorasi pada tahap implementasi (*Security Development*) [5].
2. Penelitian ini menggunakan model ChatGPT-4o karena memiliki kemampuan dalam mendukung berbagai fase dalam SDLC, seperti elisitasi kebutuhan, penulisan kode, hingga dokumentasi [5].
3. Penelitian ini mengadopsi standar keamanan dari OWASP sebagai acuan utama dalam perancangan dan pengembangan sistem, terkhusus pada sisi backend. Tiga standar utama yang digunakan meliputi OWASP *Application Security Verification Standard* (ASVS)

sebagai referensi kontrol keamanan dalam pengembangan *backend* [13], OWASP Top 10 digunakan untuk mengidentifikasi risiko atau ancaman keamanan yang paling umum terjadi pada sistem [14], dan OWASP *Secure Coding Practices* (SCP) sebagai panduan utama dalam menerapkan praktik pengkodean yang aman [15]. Ketiga ini dipilih karena menyediakan kontrol keamanan yang detail dan terstruktur, yang relevan dalam pengembangan sistem web yang aman.

4. Pengembangan sistem *backend* dilakukan dengan menggunakan pendekatan arsitektur RESTful API yang berorientasi pada modularitas dan pemisahan antara *backend* dan *frontend*. Hal ini dipilih untuk mendukung skalabilitas dan integrasi layanan kedepannya.
5. Penelitian ini bersifat eksploratif dan hanya melakukan satu kali eksperimen terhadap penggunaan Generative AI pada panduan terkait untuk meninjau bagaimana ChatGPT dapat mendukung pengembangan sistem yang aman pada sisi backend. Penelitian ini tidak melakukan perbandingan hasil dan performa pada sistem.

1.5. Metode Penelitian

Penelitian ini menggunakan metode kualitatif untuk mengkaji proses adopsi *Secure* SDLC berbasis Generative AI dalam pengembangan backend sistem layanan publik Desa Limapoccoe. Pendekatan ini dipilih karena berfokus pada eksplorasi proses, konteks dan pengembangan sistem.



Gambar 1. 1. Diagram Alur Penelitian

Proses diawali dengan studi literatur untuk mengkaji sejumlah teori dan konsep yang relevan, serta penelitian dahulu yang relevan, terutama dalam konteks Secure SDLC, standar keamanan dan peran Generative AI dalam

pengembangan sistem. Selanjutnya, identifikasi masalah dan kebutuhan dilakukan dengan wawancara terhadap masyarakat dan pemerintah desa.

Setelah kebutuhan teridentifikasi, dilakukan perancangan sistem *backend* yang mencakup *use case*, struktur API, arsitektur sistem, dan basis data. Implementasi dilakukan menggunakan *framework* Laravel 12, dengan memperhatikan kontrol keamanan dan praktik penulisan kode yang aman sesai standar keamanan.

Di tahap terakhir, yaitu analisis dan evaluasi terhadap proses pengembangan *backend*, terutama pada aspek keamanan di tahap implementasi yang dihasilkan oleh Generative AI.

1.6. Jadwal Pelaksanaan

Berikut ini adalah jadwal pelaksanaan penelitian ini sebagai berikut.

Tabel 1. 1. Jadwal Pelaksanaan Tugas Akhir

No.	Deskripsi Tahapan	1	2	3	4	5	6
1	Studi Literatur						
2	Identifikasi & Perancangan Sistem						
3	Perancangan						
4	Implementasi						
5	Analisis & Evaluasi						
6	Penyusunan Laporan/Buku TA						