BAB I
PENDAHULUAN

1.1 Latar Belakang

Multimedia adalah bentuk komunikasi berupa teks, gambar, audio, animasi, dan video yang digabungkan untuk menghasilkan output tertentu. Media-media tersebut dapat ditampilkan, disimpan, dikirim, dan diproses menggunakan berbagai perangkat [1]. Saat ini, penggunaan file multimedia semakin meningkat, sehingga kebutuhan untuk perlindungan data pada file multimedia menjadi masalah yang penting.

Perlindungan data merupakan aspek penting dalam mempertahankan kerahasiaan data, terutama data sensitif yang hanya dapat diakses oleh individu tertentu[2]. Dalam penggunaan teknologi, keamanan file multimedia menjadi hal yang sangat krusial karena data yang diunggah menggunakan jaringan publik juga diakses oleh orang lain [3]. Pada umumnya, file multimedia yang dikirimkan melalui jaringan internet tidak menerapkan proses pengamanan yang memadai. Hal ini beresiko terjadi penyadapan informasi oleh pihak yang tidak berwenang[4]. Oleh karena itu, file tersebut harus dijaga dengan tingkat keamanan dan kerahasiaan yang tinggi, karena berisi rahasia atau file berharga yang perlu diawasi agar tetap terjaga kerahasiaannya [2].

Salah satu upaya untuk memastikan keamanan file multimedia adalah melalui penerapan ilmu kriptografi. Kriptografi adalah ilmu yang berhubungan dengan keamanan informasi yang menerapkan metode enkripsi data [5]. Enkripsi adalah proses mengonversi data *plaintext*, atau teks yang dapat dimengerti oleh *user*, menjadi bentuk *ciphertext*, yakni bentuk teks atau data yang tidak dapat dipahami *user*. Dalam tahapannya, enkripsi memakai kunci kriptografi, yaitu rangkaian karakter pada algoritma enkripsi yang mampu mengubah data menjadi bentuk acak [6]. Perangkat dan aplikasi yang telah menerapkan kriptografi tentu dapat meningkatkan privasi keamanan data penggunanya [4].

Enkripsi data dengan algoritma AES (*Advanced Encryption Standard*) adalah metode yang digunakan untuk memastikan keamanan file multimedia yaitu teks, gambar, audio, dan video [7]. Algoritma AES mampu melakukan enkripsi dan dekripsi multimedia [8]. Enkripsi adalah teknik merbah data *plaintext* menjadi

ciphertext, sementara dekripsi adalah proses merubah data *ciphertext* menjadi *plaintext* [6]. Peneliti menggunakan algoritma AES (*Advanced Encryption Standard)* karena algoritma AES adalah algoritma *block cipher* yang penggunaannya lebih berhasil dibandingkan dengan algoritma *block cipher* lain [9]. Algoritma AES juga membutuhkan lebih sedikit memori dan waktu pemrosesan dibandingkan dengan algoritma DES dan RSA[10]. Algoritma AES mampu menyelesaikan tantangan perkembangan teknologi dengan sangat cepat serta terbukti lebih kuat dibandingkan dengan algoritma DES dan Triple DES [11].

Pentingnya pengamanan data untuk menjaga privasi atau kerahasiaan data terhadap file multimedia (teks, gambar, audio, video, dan animasi). Saat ini, banyak file multimedia yang tersedia di internet, sehingga dapat dimanipulasi dan dimodifikasi secara bebas tanpa mengurangi kualitas file aslinya [12]. File multimedia terutama gambar dan video sering disalah gunakan seperti kasus pencurian gambar dan video lalu digunakan untuk kepentingan komersial dan pemalsuan identitas [13].

Penelitian ini juga menerapkan metode *watermarking* untuk menjaga keamanan dan hak cipta dari file gambar dan video. Teknik *watermarking* merupakan bentuk atau implementasi dari ilmu steganografi. Steganografi adalah teknik menyembunyikan pesan rahasia pada pesan lain dan keberadaannya dibuktikan dengan proses ekstraksi [14]. Data atau pesan rahasia yang disamarkan dapat berupa teks atau gambar [15]. *Watermarking* berfungsi untuk menyamarkan kode unik pada data dengan *watermark* untuk mengidentifikasi *copy* legal dari data. Teknik *watermarking* yang digabungkan dengan kriptografi dapat meningkatkan kerahasiaan dan keamanan data [16]

Pada penelitian ini, dirancang suatu sistem untuk menjaga keamanan file gambar dan video memakai algoritma AES (*Advanced Encryption Standard*) dan teknik *watermarking*. Sistem berbasis web dirancang untuk memudahkan pengguna dalam mengakses aplikasi, karena bersifat *online* dan mendukung jika digunakan oleh banyak pengguna secara bersamaan [17]. Berdasarkan penjelasan diatas, maka penelitian ini berjudul **"Aplikasi Keamanan File Gambar dan Video menggunakan Algoritma AES (*Advanced Encryption Standard*) dan Teknik *Watermarking* berbasis WEB".**

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan, maka disusun rumusan masalah dalam penelitian ini sebagai berikut:

1. Bagaimana implementasi algoritma AES dapat membantu meningkatkan keamanan file gambar dan video berbasis web?
2. Bagaimana file yang dihasilkan setelah proses enkripsi dengan algoritma AES (*Advanced Encryption Standard*)?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah, tujuan penelitian sebagai berikut:

1. Mengimplementasikan algoritma AES (*Advanced Encryption Standard*) dan teknik *watermarking* untuk meningkatkan keamanan pada file gambar dan video berbasis web.
2. Menganalisis performa file yang dihasilkan setelah proses enkripsi menggunakan algoritma AES.

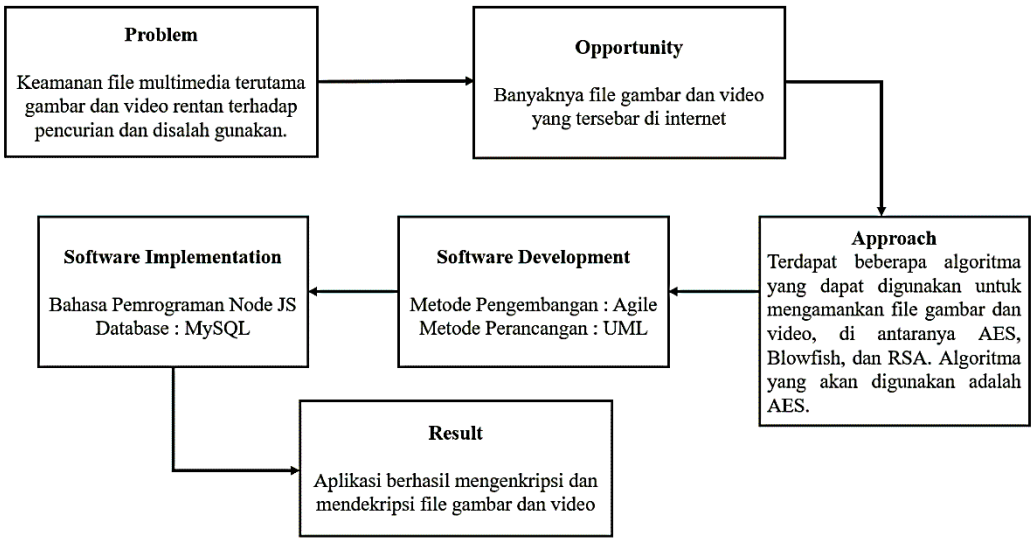
1.4 Batasan Masalah

Batasan masalah ditentukan agar penelitian ini dapat dilakukan sesuai tujuan yang diharapkan, berikut adalah beberapa batasan masalah mengenai Aplikasi Keamanan File gambar dan video menggunakan Algoritma AES (*Advanced Encryption Standard*):

1. File multimedia yang dienkripsi berupa file gambar dan video.
2. File yang dapat didownload adalah file yang berhasil di dekripsi.
3. File yang dapat di dekripsi *watermark*nya adalah file yang berhasil di dekripsi dengan kunci yang sesuai.
4. Algoritma yang diterapkan adalah AES (*Advanced Encryption Standard*).
5. File yang dapat dienkripsi berformat .jpg, .png, .mp4.
6. *Watermark* yang disisipkan pada file berupa teks.
7. Aplikasi yang dikembangkan berbasis web.

1.5 Kerangka Pemikiran

Gambar 1.1 menunjukkan kerangka pemikiran pada penelitian ini.



Gambar 1. 1 Kerangka Pemikiran

Gambar 1.1 mengilustrasikan kerangka pemikiran mengenai penelitian yang dilakukan untuk membangun aplikasi keamanan file gambar dan video dengan menerapkan algoritma AES. Algoritma AES digunakan untuk memperoleh tingkat keamanan yang kuat dan tinggi pada kunci yang dimasukkan.

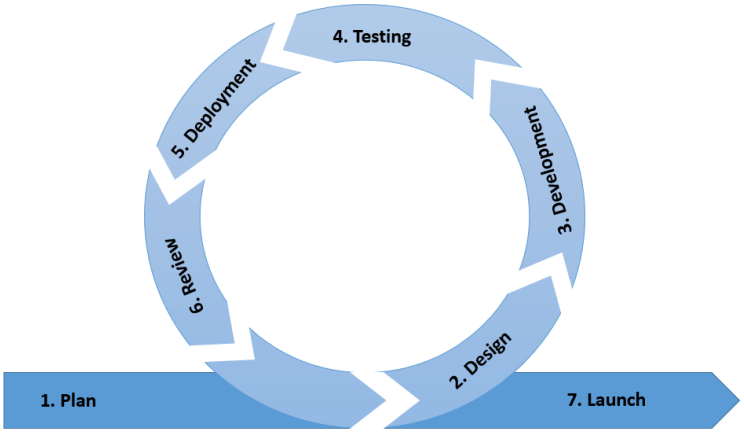
Tahapan-tahapan pengembangan perangkat lunak sebagai berikut :

1. Metode pengembangan perangkat lunak menggunakan agile.
2. Metode pemodelan aplikasi dirancang menggunakan UML (*Unified Modeling Language*)
3. Implementasi aplikasi memakai bahasa pemrograman Node JS dan *database* MySQL.

Hasil penelitian berupa aplikasi keamanan file multimedia pada file gambar dan video.

1.6 Metodologi Penelitian

Metode pengembangan yang diterapkan ketika membangun aplikasi keamanan file gambar dan video adalah metode agile. Metode agile merupakan metode yang dilakukan secara bertahap dan berulang. Metode agile digunakan karena ketika pembuatan aplikasi sedang berlangsung tetap efisien dan fleksibel terhadap perubahan yang terjadi. Berikut gambar metode pengembangan agile.



Gambar 1. 2 Metode Pengembangan

Penelitian ini dilakukan melalui beberapa tahapan diantaranya :

1. Tahap Perencanaan (*Planning*)

   Pada tahap perencanaan, peneliti mengidentifikasi kebutuhan dan merencanakan langkah-langkah untuk mencapai hasil yang diinginkan dengan studi literatur pada penelitian sebelumnya.

2. Tahap Perancangan Desain

   Pada tahap desain, peneliti merancang alur kerja aplikasi dan interaksi pengguna dengan aplikasi melalui diagram UML (*use case diagram* dan *sequence diagram*) [4].

3. Tahap Pengembangan Aplikasi (*Development*)

   Pada tahap pengembangan, peneliti mengimplementasikan algoritma AES dan teknik *watermarking* dengan pengkodean (*coding*) untuk mengembangkan aplikasi keamanan file gambar dan video menerapkan bahasa pemrograman node JS dan *database* MySQL.

4. Tahap Pengujian Aplikasi (*Testing*)

   Pada tahap pengujian, peneliti menguji aplikasi yang sudah dikembangkan menggunakan pengujian *black box*. *Black box testing* adalah teknik pengujian aplikasi dengan menekankan kinerja aplikasi tanpa memahami detail implementasi, susunan kode, dan cara kerja di dalamnya.

5. Tahap *Deployment*

   Pada tahap *deployment*, peneliti mengkonfigurasi dan mengaktifkan aplikasi yang sudah di testing ke URL di suatu server. Tahap ini dilakukan agar aplikasi dapat diakses oleh semua orang melalui URL.

6. Tahap *review*

   Pada tahap *review*, peneliti mengumpulkan umpan balik dari pengguna terkait aplikasi yang telah dikerjakan. Di tahap ini, peneliti juga melakukan perbaikan yang diperlukan berdasarkan umpan balik tersebut.

1.7 Sistematika Penulisan

Gambaran umum dan sistematis dari proses penyusunan penelitian ini, terbagi ke dalam lima bab, berdasarkan urutan berikut:

BAB I PENDAHULUAN

Bagian pendahuluan memberikan gambaran umum dari penelitian yang dilakukan, mencakup latar belakang penelitian, perumusan masalah penelitian, tujuan penelitian, batasan masalah penelitian, kerangka pemikiran penelitian, metode penelitian, dan sistematika penulisan.

BAB II KAJIAN LITERATUR

Kajian literatur berisi tinjauan pustaka dan landasan teori yang menggambarkan hasil penelitian sebelumnya dan konsep teori serta metode-metode yang sesuai untuk menyelesaikan laporan penelitian dan mengembangkan perangkat lunak.

BAB III METODOLOGI PENELITIAN

Metodologi penelitian memaparkan langkah-langkah yang diterapkan pada perancangan aplikasi yang akan dibangun serta implementasi pada aplikasi.

BAB IV HASIL DAN PEMBAHASAN

Bab implementasi menguraikan dua aspek utama yaitu implementasi dan pengujian. Pada bab implementasi juga, ditampilkan UI dari sistem yang sudah dirancang.

BAB V KESIMPULAN DAN SARAN

Bab ini mencakup kesimpulan dari penjelasan pada bab I sampai dengan bab V, serta memberikan rekomendasi saran untuk pengembangan penelitian.