# BAB I PENDAHULUAN

## Latar Belakang

Pada era *Society 5.0* yang merupakan perkembangan dari era *Industry 4.0*, media sosial sudah menjadi kebutuhan pokok bagi semua orang. Kebutuhan akan informasi setiap individu menjadi sangat besar karena berkembang pesatnya aplikasi media sosial seperti *Facebook*, *WhatsApp*, *Line*, *Messenger*, *Twitter*, dan lainnya, informasi macam apapun kemungkinan ada di situ karena setiap hal yang dikirim atau di-*post* sudah pasti diawasi oleh perusahaan pendiri aplikasi tersebut. Namun, dalam perkembangannya, tidak semua pengguna paham betul konsep keamanan informasi/privasi mereka.

Kekurangan pada struktur database sosial media konvensional adalah menggunakan database fisik untuk urusan penyimpanan data penggunanya. Oleh karena itu, keamanan pada penyimpanan fisik menjadi banyak faktor, pertama faktor internal, walaupun sekalipun suatu perusahaan menggunakan kualitas database server yang sangat bagus, tidak nol kemungkinan bahwa alat tersebut butuh perbaikan/rusak sebagian, dalam hal ini tentu pelayanan dari server tersebut harus dilakukan pemberhentian sementara untuk perbaikan/*maintenance*. Pada faktor eksternal, serangan hacker dapat menyebabkan kerusakan pada pelayanan, serangan semacam *SQL Injection* & *Cross-Site Scripting (XSS)* dapat merusak data yang ada didalamnya secara keseluruhan, dan serangan semacam *Man in the Middle* dapat mencuri data dari dua orang yang saling berkomunikasi.

Dalam penggunaan database terdesentralisasi, database fisikal tidak diperlukan lagi. Dalam penyimpanan data, database terdesentralisasi Gun.js menggunakan teknologi WebRTC dalam penyimpanannya, terdistribusi keseluruh pengguna/*peer.* Data yang tersimpan dimasing-masing local storage browser milik pengguna disinkronisasi setiap ada perubahan dengan data yang berada di pengguna lain atau pada *relay server* yang di *deploy* untuk membuat sistem lebih stabil. Sehingga artinya, seluruh database adalah suatu kesatuan dari seluruh pengguna. Keunggulan penggunaan database terdesentralisasi ini adalah *realtime update*, *offline mode* dan *latency compensation*. Data yang tersimpan tersebut diatur dalam bentuk *minimal graph API* yang dimana setiap *record* adalah sebuah *node* yang memiliki ID unik untuk masing-masing, artinya setiap interaksi dari setiap *node* akan menghubungkan *node* satu dengan yang lainnya.

Dengan demikian, keamanan privasi pengguna akan semakin sulit untuk diretas, *maintenance* fisikal dan semacamnya juga tidak diperlukan. Pada Gun.JS terdapat fitur *SEA (Security, Encryption & Authentication)*. Yang artinya percakapan antara dua pengguna sangat tidak mungkin diinterupsi/dicuri dipertengahan saat pengiriman pesan.

## Rumusan Masalah

1. Apa sejarah awal pertukaran pesan *(message services)*?
2. Apa itu GunJS? Fitur apa saja yang ditawarkan?
3. Bagaimana struktur dan cara kerja database konvensional
4. Bagaimana arsitektur aplikasi percakapan dengan database konvensional?
5. Bagaimana struktur dan cara kerja database terdesentralisasi?
6. Bagaimana arsitektur aplikasi percakapan dengan database terdesentralisasi?
7. Serangan seperti apa saja yang mungkin dilakukan untuk menginterupsi layanan? Fitur keamanan apa saja yang ditawarkan?

## Maksud dan Tujuan Penelitian

1. Mengetahui sejarah awal pertukaran pesan atau *message services* diseluruh dunia.
2. Mengetahui secara jelas library GunJS dengan segala fitur yang tersedia.
3. Mengetahui bentuk struktur dan cara kerja database konvensional.
4. Mengetahui struktur aplikasi percakapan dengan menggunakan database konvensional.
5. Mengetahui bentuk struktur dan cara kerja database terdesentralisasi.
6. Mengetahui dan dapat membuat arsitektur aplikasi percakapan dengan menggunakan teknologi database terdesentralisasi.
7. Mengetahui segala jenis serangan cyber yang dapat terjadi pada aplikasi dalam hal peretasan layanan, dan mengetahui fitur keamanan apa saja yang dapat menangkal hal tersebut.

## Pembatasan Masalah

1. Pengguna dummy dan sedikit
2. Sistem yang masih dalam masa perkembangan dan belum *production ready*
3. *Resource* yang terbatas

## Manfaat Penelitian

1. Peningkatan keamanan privasi pengguna sosial media
2. Mengurangi biaya *maintenance* pada database fisikal
3. Penggunanaan teknologi terbaru pada aplikasi percakapan yang *mainstream*

## Metode Penelitian

Metode yang digunakan pada penelitian proyek akhir ini adalah:

1. Studi Literatur

Metode ini dilakukan dengan membaca keseluruhan dokumentasi library GunJS dan dokumentasi teknologi pelengkap lainnya dari berbagai sumber yang tersedia dan berhubungan langsung dengan permasalahan yang dibahas pada proyek akhir ini.

1. Praktik

Metode ini dilakukan dengan cara mengimplementasikan langsung bacaan dari studi literatur kedalam *source code*.

1. Evaluasi

Metode ini dilakukan untuk melakukan *review* atau pembahasan dari hasil penelitian.

## Sistematika Penulisan

Sistematika penulisan yang digunakan pada proyek akhir ini adalah sebagai berikut:

**BAB I PENDAHULUAN**

Pada bab ini berisi segala informasi dasar yang dibutuhkan dalam penelitian, seperti latar belakang, rumusan masalah, maksud dan tujuan penelitian, pembatasan masalah, metode penelitian dan sistematika penulisan yang digunakan.

**BAB II LANDASAN TEORI**

Pada bab ini menjelaskan pengertian tentang segala teori yang berhubungan dengan masalah pada proyek akhir ini.

**BAB III METODE PENGAMBILAN DATA**

Pada bab ini menjelaskan tentang persiapan dan metode apa saja yang dibutuhkan untuk pengambilan, pengumpulan dan penggunaan data.

**BAB IV RANCANG BANGUN APLIKASI**

Pada bab ini menjelaskan tata cara dalam pembuatan aplikasi lengkap dengan segala teori dan data yang didapatkan di bab sebelumnya.

**BAB V PENUTUP**

Pada bab ini berisi kesimpulan atas penelitian yang dilakukan dan hasil akhir dari aplikasi yang dibuat.