A. Latar Belakang

Hampir seluruh perangkat saat ini terhubung dengan internet, seperti *smartphone*, komputer, dan *smart TV*. Meskipun tekonologi internet sangatlah bermanfaat, tetapi teknologi ini juga menimbulkan ancaman keamanan.

Dari survey yang dilakukan, mayoritas developer tidak ragu melakukan *personalized-ads*. Jenis iklan ini menggunakan data pengguna untuk memilihkan iklan yang dianggap relevan berdasarkan data pengguna. Hal ini tidak mengherankan karena jenis iklan ini menawarkan pendapatan yang lebih tinggi dibandingkan iklan biasa, karena peluang pengguna membuka iklan yang ditawarkan lebih besar(**tahaei2021**). Penelitian lain juga menunujukkan bahwa 77% aplikasi Android gratis menggunakan *ad library*(**he2018**; **jin2021**).

Hal ini akan menjadi masalah ketika pihak yang mengumpulkan data tersebut mengalami kebocoran atau bahkan menggunakannya untuk hal-hal yang melanggar etika.

Iklan-iklan yang ditampilkan sering kali sangat intrusif dan menggangu. Contohnya seperti iklan yang menutupi konten, iklan melalui *pop-up*, atau iklan yang otomatis mengarahkan pengunjung ke *tab* baru yang memuat iklan. Atau bahkan menampilkan iklan yang menjurus ke arah konten dewasa.

Masalah lain selain iklan yang mengganggu, adalah masalah keamanan. Banyak layanan yang memasang iklan juga menggunakan layanan *web analytics* untuk melakukan *tracking* terhadap pengunjung atau penggunanya. Layanan web analytics inilah yang dapat menjadi celah keamanan. Contohnya pada tahun 2019, layanan Google Analytics digunakan untuk mengiklankan website phising(**charlie2019**). Sedangkan di tahun 2020, peretas memasukkan kode berbahaya ke dalam website yang diretas, yang mana kode tersebut mengumpulkan informasi kredit pengguna dan mengirimkannya menggunakan Google Analytics, kemudian peretas akan mengakses data kredit yang dikumpulkan di akun Google Analytics miliknya(**ravie2020**).

Hal-hal tersebut bisa dicegah dengan menggunakan metode DNS *ad-blocking*, dengan metode ini, kita bisa melakukan pemblokiran domain yang melakukan *tracking*, domain yang digunakan sebagai tempat menyimpan kode JavaScript yang berbahaya, atau domain milik penyedia iklan. Tetapi metode ini hanya bisa melakukan pemblokiran berdasarkan nama domain, sehingga jika iklan atau kode JavaScript berada pada domain yang sama dengan website utama, maka kita

harus mengizinkan iklan, dan kode JavaScript berjalan, atau memblokir domain website tersebut sehingga tidak bisa diakses.

Metode lain adalah menggunakan *add-on* peramban, seperti *UBlock Origin*. Metode ini mampu melakukan *blocking* terhadap iklan atau kode JavaScript yang berbahaya, walaupun keduanya berada pada domain yang sama dengan website utama. Sayangnya *add-on* ini hanya bisa di-*install* pada peramban tertentu, seperti Mozilla Firefox, dan Chrome Desktop.

Berdasarkan permasalahan yang disebutkan di atas, tujuan saya adalah membangun sistem HTTPS filtering dengan menggunakan MITM-Proxy. Sistem ini bertujuan untuk menyaring konten yang tidak diinginkan agar tidak diakses.

Filtering dengan menggunakan MITM-Proxy saya pilih karena tools ini merupakan proxy, sehingga bisa digunakan di banyak perangkat seperi metode DNS *ad-blocking*, tetapi bisa di buat sedemikian rupa dengan menuliskan *script* Python sehingga mampu melakukan filtering seperti *add-on* pada browser, atau bahkan melebihinya.

Selain itu kelebihan MITM-Proxy yang lain adalah software ini bersifat *open source* dan gratis. Software ini bisa digunakan sebagai alat untuk mencegat, inspeksi, dan memodifikasi lalu lintas web, seperti HTTP/1, HTTP/2, WebSockets, atau protokol lainnya yang dilindungi oleh SSL/TLS.