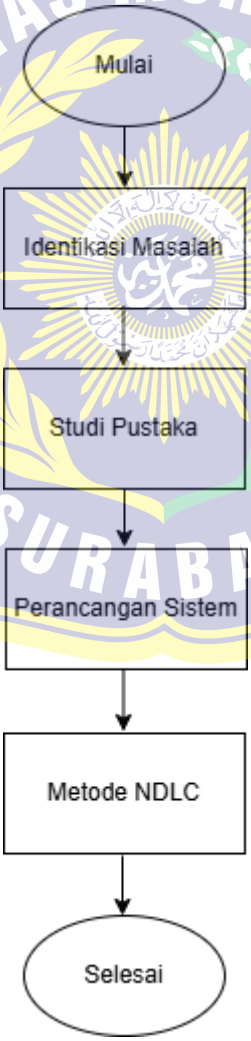
BAB III
METODOLOGI PENELITIAN

3.1 Tahapan Penelitian

Penelitian ini menggunakan metode *Network development life cycle* (*NDLC*) sebagai kerangka kerja dalam pengembangan sistem pembatasan akses internet berbasis ekstensi *browser* (Nengsi S., 2025). Pemilihan metode *NDLC* didasarkan pada karakteristik penelitian yang berfokus pada perancangan dan implementasi sistem jaringan serta pengelolaan keamanan akses internet di lingkungan perguruan tinggi, untuk itu dilakukan dengan beberapa tahapan alur yang harus disiapkan untuk penelitian antara lain, sebagai berikut:



Gambar 3.1 Flowchart Penelitian

Pada gambar 3.1 Flowchart penelitian menggambarkan tahapan penelitian yang dilaksanakan secara sistematis dengan mengacu pada metode *Network development life cycle* (*NDLC*). Alur ini menunjukkan keterkaitan antar tahapan penelitian mulai dari identifikasi permasalahan hingga evaluasi dan penyelesaian penelitian. Penelitian diawali dengan tahap mulai, yang menandai dimulainya seluruh rangkaian proses penelitian. Pada tahap ini, peneliti menetapkan fokus penelitian yang berkaitan dengan pembatasan akses internet berbasis ekstensi *browser* di lingkungan UMSURA.

Tahap berikutnya adalah identifikasi masalah, yang bertujuan untuk mengenali dan merumuskan permasalahan utama yang menjadi latar belakang penelitian. Pada tahap ini ditemukan bahwa akses internet yang bersifat terbuka memungkinkan pengguna mengakses laman dan konten yang tidak sesuai dengan tujuan akademik. Permasalahan ini menjadi dasar perlunya pengembangan sistem pembatasan akses internet yang lebih terarah dan fleksibel.

Setelah permasalahan teridentifikasi, penelitian dilanjutkan dengan studi pustaka. Tahap ini dilakukan untuk mengumpulkan dan mempelajari referensi yang relevan, baik berupa buku, jurnal ilmiah, maupun penelitian terdahulu yang berkaitan dengan *web* content filtering, ekstensi *browser*, serta metode *NDLC*. Studi pustaka berfungsi sebagai landasan teoritis dalam menentukan pendekatan, metode, dan solusi yang akan digunakan dalam penelitian.

Tahap pertama adalah analisis, yang bertujuan untuk menentukan kebutuhan sistem secara lebih rinci. Pada tahap ini dilakukan analisis terhadap fungsi sistem yang dibutuhkan, seperti pemblokiran laman berbasis *domain*, penyensoran konten berbasis kata kunci, serta pencatatan *log* aktivitas. Hasil analisis menjadi acuan utama dalam proses perancangan sistem. Tahap selanjutnya adalah desain, yaitu perancangan arsitektur dan alur kerja sistem pembatasan akses internet. Pada tahap ini dirancang hubungan antara ekstensi *browser* sebagai komponen utama pembatasan akses dengan *web*site administrator sebagai pusat pengelolaan kebijakan. Perancangan dilakukan untuk memastikan

bahwa sistem dapat berjalan secara terintegrasi dan sesuai dengan kebutuhan yang telah dianalisis sebelumnya.

Setelah tahap desain, dilakukan simulasi untuk menguji rancangan sistem secara awal. Simulasi bertujuan untuk memastikan bahwa alur sistem telah sesuai dengan rancangan dan dapat berjalan dengan baik sebelum diterapkan secara penuh. Pada tahap ini juga dilakukan identifikasi terhadap potensi kekurangan atau kelemahan sistem yang mungkin muncul. Berdasarkan hasil simulasi, penelitian dilanjutkan ke tahap implementasi, yaitu penerapan sistem pembatasan akses internet berbasis ekstensi *browser* secara nyata. Pada tahap ini dilakukan pengembangan ekstensi *browser*, pembuatan *web*site administrator, serta integrasi antar komponen sistem sehingga sistem dapat digunakan sesuai dengan tujuan penelitian.

Tahap monitoring dilakukan setelah sistem diimplementasikan untuk mengamati kinerja sistem secara berkelanjutan. Monitoring difokuskan pada efektivitas pemblokiran laman, penyensoran konten, serta keakuratan pencatatan *log* aktivitas sistem. Data hasil monitoring digunakan sebagai bahan evaluasi terhadap kinerja sistem.

3.2 Kebutuhan Sistem

Kebutuhan sistem pada penelitian ini dibagi menjadi dua bagian utama, yaitu kebutuhan perangkat lunak (*software*) dan kebutuhan perangkat keras (*hardware*). Penentuan kebutuhan sistem bertujuan untuk memastikan bahwa proses perancangan, implementasi, dan pengujian sistem pembatasan akses internet berbasis ekstensi *browser* dapat berjalan dengan baik disesuaikan dengan studi kasus yang menjadi tempat penelitian .

3.2.1 Kebutuhan Perangkat Lunak (Sofware)

Perangkat lunak yang digunakan dalam penelitian ini berfungsi sebagai pendukung utama dalam pengembangan dan pengujian sistem UMSURA *SHIELD*. Pemilihan perangkat lunak disesuaikan dengan kebutuhan sistem, kemudahan penggunaan, serta kompatibilitas antar komponen sistem.

Tabel 3.1 Software yang digunakan

NO	Software	Fungsi
1.	Google Chrome	Sebagai media instalasi dan pengujian ekstensi *browser*.
2.	*Javascript*	Bahasa pemrograman untuk pengembangan ekstensi *browser*.
3.	*PHP*	Bahasa pemrograman untuk *web*site administrator dan *API*.
4.	*MysQl*	Sistem manajemen basis data untuk penyimpanan data.
5.	Apache *Web* Server	Menjalankan *web*site administrator dan layanan *API*.
6.	XAMPP	Paket server lokal (*Apache*, *PHP*, *MysQl*)
7.	Visual Studio Code	Text editor untuk penulisan dan pengelolaan kode.

3.2.2 Kebutuhan Perangkat Keras (Hardware)

Perangkat keras yang digunakan mendukung proses pengembangan, implementasi, serta pengujian sistem. Spesifikasi perangkat keras yang digunakan disesuaikan dengan kebutuhan minimum agar sistem dapat berjalan secara optimal.

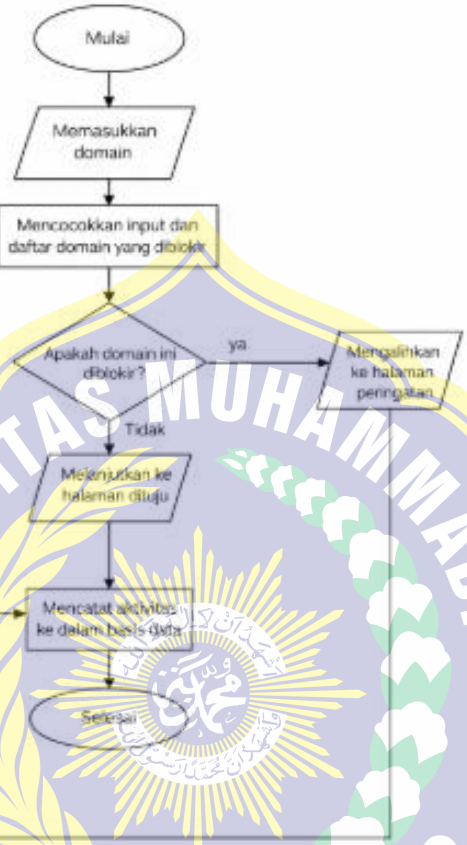
Tabel 3.2 Hardware yang digunakan

NO	Hardware	Fungsi
1.	Laptop / PC	Pengujian sistem dengan spesifikasi minimal Prosesor minimal Intel Core i3, RAM 8 GB, penyimpanan 256 GB
2.	Server Lokal / Kampus	Menjalankan *web*site administrator dan *database*.
3.	Perangkat *Client*	Laptop atau PC pengguna dengan *browser* terpasang ektensi.

3.3 Perancangan sistem

3.3.1 Perancangan Pemblokiran Domain

Fitur pemblokiran *domain* berjalan dengan mengalihkan *domain* tertentu ke halaman lain. Tahapan yang dilakukan ditunjukkan pada Gambar 3.2



Gambar 3.2 Metode Pemblokiran *Domain*

Gambar 3.2 tersebut menggambarkan alur kerja fitur pemblokiran *domain* yang diterapkan pada sistem UMSURA *SHIELD* berbasis ekstensi *browser*. Proses ini dimulai ketika pengguna mencoba mengakses suatu halaman *web* melalui *browser* yang telah terpasang ekstensi UMSURA *SHIELD*. Setiap permintaan akses halaman *web* akan d*ip*antau oleh ekstensi *browser* secara otomatis sebelum halaman tersebut ditampilkan kepada pengguna.

Pada tahap awal, sistem menerima input berupa *domain* tujuan yang akan diakses oleh pengguna. *domain* ini kemudian dicocokkan dengan daftar *domain* terblokir yang telah ditetapkan oleh administrator melalui *web*site pengelolaan

sistem. Daftar *domain* terblokir tersebut disimpan dalam file konfigurasi *rules.json* yang dibaca langsung oleh ekstensi *browser*, sehingga kebijakan pemblokiran dapat diterapkan secara cepat tanpa bergantung pada proses *query database* secara langsung.

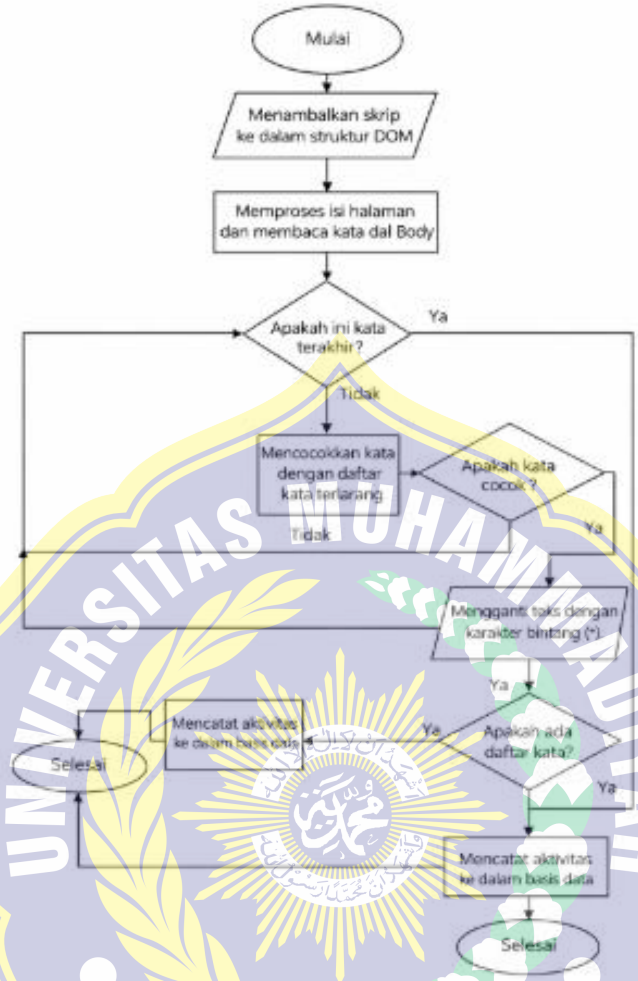
Selanjutnya, sistem melakukan proses pencocokan *domain*. Apabila *domain* yang diakses oleh pengguna termasuk dalam daftar *domain* terblokir, maka sistem akan langsung menghentikan proses akses dan mengalihkan pengguna ke halaman peringatan. Halaman ini berfungsi sebagai notifikasi bahwa *domain* yang diakses tidak diperbolehkan sesuai kebijakan pembatasan akses internet yang berlaku di lingkungan UMSURA. Pengalihan ini dilakukan di sisi pengguna *(client-side)* melalui mekanisme ekstensi *browser*.

Selain melakukan pemblokiran, sistem juga menjalankan proses pencatatan *log* aktivitas pemblokiran *domain*. Ketika terjadi pemblokiran, ekstensi *browser* akan mengirimkan data kejadian tersebut ke server melalui *Application Programming Interface (API) (Mukharil Bachtiar et al., 2024)*. Data yang dikirimkan meliputi *domain* yang diblokir dan informasi waktu akses, sedangkan alamat *IP* pengguna diperoleh secara otomatis pada sisi server. Data ini kemudian disimpan ke dalam *database* dan ditampilkan pada menu *log* blokir *web* pada *web*site administrator sebagai bahan monitoring dan evaluasi.

Pembatasan akses internet pada sistem UMSURA *SHIELD* difokuskan pada pemblokiran domain tertentu pada konten halaman web yang diakses pengguna (Nuwairah et al., 2024). Pendekatan ini dipilih karena pemfilteran berbasis domain dinilai lebih ringan, responsif, dan efektif untuk diterapkan pada lingkungan pendidikan dibandingkan pemblokiran berbasis jaringan secara menyeluruh. Penelitian menunjukkan bahwa content filtering berbasis teks dan URL mampu menekan akses terhadap konten negatif tanpa mengganggu akses ke sumber informasi akademik yang sah, serta tidak memerlukan perubahan konfigurasi infrastruktur jaringan yang kompleks.

3.3.2 Perancangan Penyensoran Kata

Fitur penyensoran kata berjalan dengan mengalihkan *domain* tertentu ke halaman lain. Tahapan yang dilakukan ditunjukkan pada Gambar 3.3



Gambar 3.3 Metode Penyensoran Kata

Gambar 3.3 tersebut menggambarkan Alur kerja sistem penyensoran kata pada gambar tersebut dimulai dari proses Mulai, ketika ekstensi atau *script* sensor dijalankan pada halaman *web* yang diakses pengguna. Sistem kemudian memasukkan scr*ip*t ke dalam *DOM (Document Object Model)*, sehingga *script* dapat membaca dan memproses seluruh konten teks yang ada di halaman *web* (Wang & Liu, 2022). Setelah itu, sistem memproses dan menghitung jumlah kata di dalam *body* halaman, yang bertujuan untuk mengetahui seluruh teks yang akan dianalisis satu per satu.

Selanjutnya, sistem masuk ke proses perulangan *(while)* untuk memeriksa setiap kata. Pada setiap iterasi, sistem mengecek apakah kata yang sedang diproses merupakan kata terakhir (Rahmat et al., 2022). Jika belum, sistem akan melakukan pencocokan antara kata input (teks halaman) dengan daftar kata terlarang yang telah disimpan sebelumnya. Apabila hasil pencocokan menunjukkan kata tidak cocok, sistem akan melanjutkan ke kata berikutnya. Namun jika kata cocok dengan daftar kata terlarang, maka sistem akan mengganti kata tersebut dengan karakter bintang (*) sesuai panjang kata, sehingga makna kata disamarkan tanpa mengubah struktur teks halaman.

Fitur penyensoran kata UMSURA SHIELD tidak hanya bekerja berdasarkan pencocokan kata secara langsung, tetapi juga mengacu pada klasifikasi kata-kata terlarang berdasarkan elemen konten. Klasifikasi ini bertujuan untuk membuat proses penyensoran lebih terstruktur, terfokus, dan sesuai dengan norma dan etika akademik di pendidikan tinggi (Zikrina & Fitriyani, 2025).

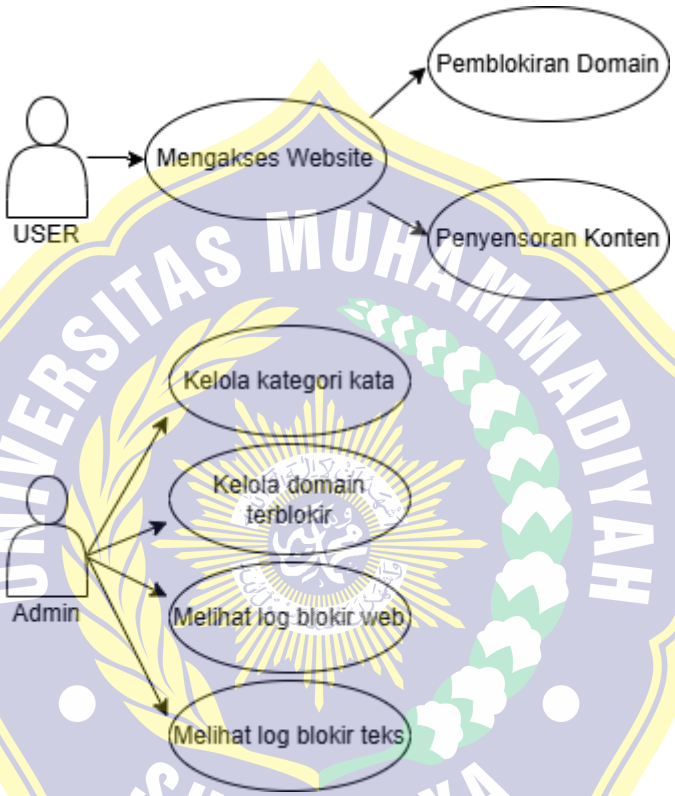
Tabel 3.3 Klasifikasi Kata Terlarang

No	Kategori Kata	Contoh Kata	Alasan Pemblokiran
1	Pornografi	Kata bermuatan seksual	Tidak sesuai etika akademik
2	Rasisme	penghinaan SARA	Menimbulkan konflik sosial
3	Kekerasan	ancaman, provokasi	Mengganggu kenyamanan
4	Sarkasme / Ujaran Kebencian	hinaan kasar	Tidak mendidik
5	Judi	taruhan, kasino	Melanggar norma hukum

Daftar kata terlarang yang digunakan dalam proses pencocokan pada Tabel 3.3 dikelompokkan ke dalam beberapa kategori, antara lain pornografi, rasisme, ujaran kebencian, kekerasan, dan kata tidak pantas. Pengelompokan ini dilakukan oleh administrator melalui website pengelolaan sistem, sehingga setiap kata yang disimpan dalam basis data memiliki dasar klasifikasi yang jelas. Pendekatan ini sejalan dengan penelitian terkait klasifikasi konten negatif yang menyatakan bahwa pemfilteran berbasis kategori mampu meningkatkan efektivitas penyaringan teks pada halaman web.

3.3.1 Use case

Use case Diagram pada penelitian ini menggambarkan interaksi antara administrator dan pengguna dalam sistem UMSURA *SHIELD*, di mana administrator berperan dalam pengelolaan kebijakan pembatasan akses internet, sedangkan pengguna berinteraksi secara tidak langsung melalui proses pemblokiran *domain* dan penyensoran konten yang dilakukan oleh sistem (Ramdany et al., n.d.).



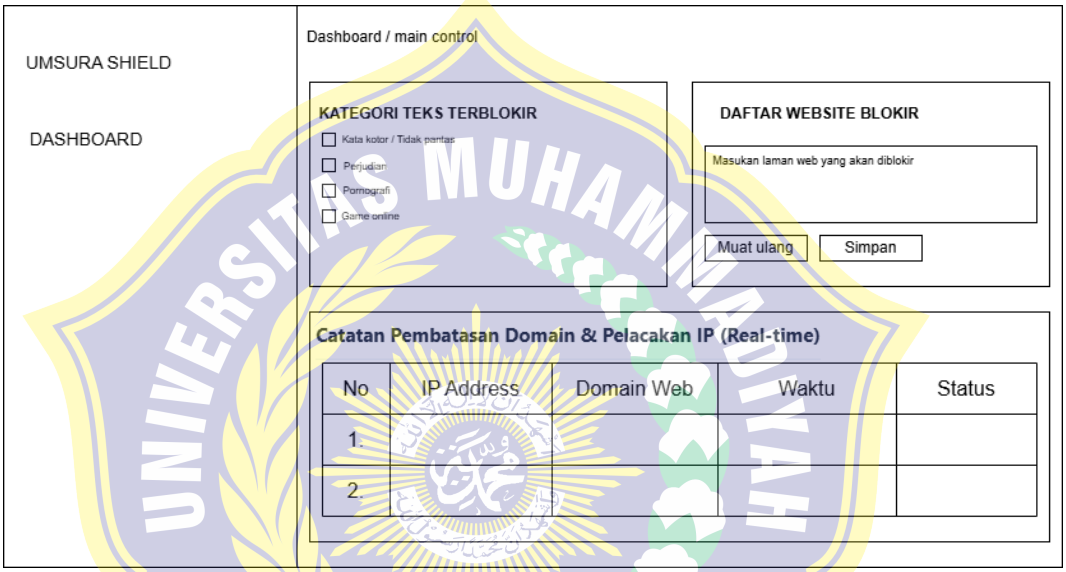
Gambar 3.4 *Use case* Diagram

Use case Diagram pada penelitian ini menggambarkan interaksi antara Administrator dan Pengguna dalam sistem pembatasan akses internet berbasis ekstensi *browser* UMSURA *SHIELD*. Administrator berperan dalam mengelola kebijakan sistem, seperti pengelolaan kategori kata, *domain* terblokir, serta pemantauan aktivitas melalui *log* blokir *web* dan *log* blokir teks. Kebijakan yang ditetapkan oleh administrator menjadi acuan utama bagi sistem dalam menjalankan fungsi pembatasan akses internet.

Pengguna merupakan pihak yang menggunakan *browser* dengan ekstensi UMSURA *SHIELD* untuk mengakses *web*site. Setiap aktivitas akses yang dilakukan pengguna akan di*p*roses secara otomatis oleh sistem, termasuk pemeriksaan *domain* dan konten halaman *web*. Apabila ditemukan *domain* terblokir atau kata yang termasuk kategori terlarang, sistem akan melakukan pemblokiran atau penyensoran sesuai kebijakan yang berlaku.

3.3.2 Interface

a. Tampilan Website



Gambar 3.5 Tampilan halaman *web*site

Gambar 3.5 *Dashboard* UMSURA *SHIELD* merupakan halaman utama pada *web*site administrator yang berfungsi sebagai pusat kendali dalam pengelolaan sistem pembatasan akses internet berbasis ekstensi *browser*. Melalui halaman ini, administrator dapat mengatur kategori konten yang diblokir serta menentukan *domain web*site yang dibatasi aksesnya. Seluruh pengaturan tersebut dikelola secara terpusat sehingga kebijakan pembatasan dapat diterapkan secara konsisten pada komputer Lab.Terpadu UMSURA.

Selain sebagai media pengelolaan, *dashboard* juga berfungsi sebagai sarana monitoring sistem. Administrator dapat melihat catatan aktivitas pemblokiran *domain* secara *real-time* yang menampilkan informasi alamat *IP* pengguna,

domain yang diblokir, waktu kejadian, dan status pemblokiran. Informasi ini digunakan untuk mengevaluasi efektivitas kebijakan pembatasan akses internet serta memastikan sistem UMSURA *SHIELD* berjalan sesuai dengan tujuan penelitian.

b. Tampilan domain yang terblokir

Gambar 3.6 Tampilan *domain* yang berhasil diblokir

Interface pada gambar menampilkan halaman peringatan pemblokiran *domain* yang dihasilkan oleh sistem UMSURA *SHIELD* ketika pengguna mengakses *web*site yang termasuk dalam daftar blokir. Halaman ini berfungsi sebagai notifikasi bahwa akses ke *web*site tersebut dibatasi sesuai kebijakan yang telah ditetapkan oleh administrator. Informasi yang ditampilkan disusun secara sederhana dan jelas untuk memberikan pemahaman kepada pengguna mengenai alasan pemblokiran, sekaligus mengarahkan pengguna untuk menutup tab atau beralih ke halaman lain, sehingga proses pembatasan akses internet dapat berjalan secara efektif tanpa menimbulkan kebingungan pada pengguna.

3.4 Rencana Evaluasi

Evaluasi sistem pada penelitian ini bertujuan untuk memastikan bahwa UMSURA *SHIELD* berfungsi sesuai dengan rancangan dan kebutuhan penelitian. Evaluasi dilakukan melalui pengujian fungsionalitas utama, yaitu pemblokiran *domain* *web*site dan penyensoran konten berbasis kategori kata. Pengujian dilakukan dengan mengakses *domain* dan konten yang telah ditetapkan dalam kebijakan sistem untuk memastikan ekstensi *browser* mampu memblokir akses serta menampilkan halaman peringatan sesuai dengan aturan yang telah ditentukan.

Selain itu, evaluasi juga dilakukan terhadap pencatatan *log* dan kinerja sistem. Pengujian *log* bertujuan untuk memastikan setiap aktivitas pemblokiran *domain* dan penyensoran konten tercatat dengan baik, termasuk informasi alamat *IP* pengguna, *domain* yang diblokir, dan waktu kejadian. Evaluasi kinerja dilakukan untuk memastikan penerapan pembatasan akses tidak mengganggu aktivitas browsing pada *web*site yang diperbolehkan, sehingga sistem dapat digunakan secara efektif di lingkungan UMSURA.