

BAB I

PENDAHULUAN

1.1 Latar Belakang

Di era digital yang terus berkembang, keamanan jaringan menjadi aspek yang sangat penting dalam pengelolaan infrastruktur teknologi informasi. Dengan meningkatnya penggunaan internet di berbagai sektor, termasuk pendidikan, ancaman terhadap keamanan siber semakin kompleks dan beragam. Sekolah sebagai lembaga pendidikan menghadapi tantangan besar dalam mengontrol akses ke situs-situs yang tidak pantas bagi siswa, seperti situs berbahaya atau yang tidak sesuai dengan kebijakan yang ditetapkan. Dalam konteks ini, *administrator* jaringan dihadapkan pada tantangan utama dalam mengelola akses pengguna ke situs-situs tersebut dan memastikan bahwa kebijakan jaringan diterapkan dengan baik. Tanggung jawab utama *administrator* jaringan adalah untuk mengelola akses pengguna ke sumber daya jaringan, termasuk situs web, serta memastikan bahwa semua aktivitas jaringan sesuai dengan kebijakan yang telah ditetapkan. Mereka berperan sebagai penjaga gerbang yang menentukan siapa saja yang dapat mengakses situs tertentu dan memastikan bahwa aktivitas *online* berjalan sesuai dengan aturan yang ada (Sidik et al., 2023).

Tantangan ini tidak hanya dihadapi oleh institusi pendidikan seperti sekolah, tetapi juga oleh berbagai sektor lainnya, termasuk pemerintahan dan bisnis. Keamanan jaringan komputer merupakan elemen penting dalam pengelolaan teknologi di berbagai sektor. Seiring dengan perkembangan teknologi dan meningkatnya penggunaan internet, jaringan komputer menjadi lebih rentan terhadap berbagai ancaman keamanan. Oleh karena itu, penting untuk menerapkan

strategi keamanan yang efektif guna melindungi informasi dan sistem dari potensi serangan siber (Widianto et al., 2024).

Seiring dengan perkembangan teknologi informasi dan meningkatnya penggunaan internet, jaringan komputer menjadi semakin rentan terhadap berbagai ancaman keamanan. Menurut Saputra et al., (2023), keamanan jaringan sangat penting untuk menjaga integritas, kerahasiaan, dan ketersediaan informasi di dalam sebuah sistem. Keamanan jaringan komputer melibatkan upaya perlindungan dari akses tidak sah, pencurian data, hingga serangan siber seperti *malware* dan *ransomware*, yang bertujuan untuk memastikan bahwa informasi yang tersimpan tetap aman.

Pentingnya keamanan jaringan semakin disoroti oleh data dari laporan terbaru *We Are Social* yang berjudul "Digital 2023: Indonesia." Laporan tersebut mengungkapkan bahwa jumlah pengguna internet di Indonesia per Januari 2023 telah mencapai 212,9 juta jiwa atau setara dengan 77.0% dari total populasi, meningkat sebesar 5,2% dari tahun sebelumnya. Meski peningkatan ini membawa dampak positif, seperti kemudahan akses informasi dan komunikasi, tantangan terkait keamanan siber juga semakin meningkat seiring dengan literasi digital yang belum merata.

Keamanan jaringan tidak hanya sebatas perlindungan terhadap ancaman siber dari luar, tetapi juga mencakup upaya untuk menjaga kebijakan internal sebuah organisasi atau institusi pendidikan, terutama dalam hal mengelola akses terhadap situs-situs berbahaya. Di Indonesia, kerangka hukum yang mengatur keamanan informasi telah diatur melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan revisinya pada UU

Nomor 19 Tahun 2016. Pasal 30 UU ITE menyatakan bahwa setiap orang yang mengakses komputer dan/atau sistem elektronik tanpa izin dapat dikenai pidana. Keberadaan UU ini penting untuk mendorong penerapan standar keamanan jaringan, khususnya di sektor pendidikan dan bisnis, guna melindungi infrastruktur digital dari ancaman siber yang semakin kompleks.

Badan Siber dan Sandi Negara (BSSN) dalam laporannya tahun 2023 mencatat lebih dari 976 juta trafik anomali sepanjang tahun 2022 di Indonesia. Temuan ini menunjukkan bahwa pendekatan keamanan tradisional, seperti hanya mengandalkan firewall, tidak lagi memadai dalam menghadapi serangan yang semakin kompleks. Oleh karena itu, diperlukan sistem yang adaptif dan tahan terhadap berbagai bentuk gangguan, yakni melalui pendekatan keamanan berlapis (*defense in depth*).

Menurut Prasanth dan Pothiraj (2024), sistem keamanan modern harus menerapkan kerangka yang terdiri dari beberapa lapisan fungsional, seperti pengumpulan data, analisis anomali, serta respons otomatis dengan kecerdasan buatan. Mereka menyatakan bahwa “arsitektur berlapis-lapis ini memfasilitasi pendekatan komprehensif terhadap keamanan siber, memastikan bahwa organisasi dapat mengelola ancaman secara efektif dalam waktu nyata.” Dengan pendekatan ini, sistem mampu mendeteksi lebih awal, mengisolasi ancaman, dan merespons dengan cepat sebelum kerusakan meluas. Jika satu lapisan gagal, lapisan lainnya tetap dapat melindungi sistem, menjadikan keamanan berlapis sebagai bentuk nyata dari implementasi keamanan jaringan yang efektif di era digital.

Keamanan berlapis adalah konsep keamanan informasi yang berfokus pada ide bahwa pertahanan yang kokoh terhadap ancaman dapat dicapai dengan

menerapkan berbagai lapisan keamanan. Teori Keamanan Berlapis menekankan pentingnya tidak hanya mengandalkan satu mekanisme keamanan, melainkan menerapkan sejumlah lapisan pertahanan (Hoshmand & Ratnawati, 2023). Pendekatan ini menggabungkan beberapa lapisan keamanan, sehingga jika satu lapisan gagal, lapisan lainnya masih dapat memberikan perlindungan.

Di sektor pendidikan, penerapan keamanan berlapis menjadi sangat relevan dalam melindungi jaringan sekolah dari akses ilegal dan ancaman situs berbahaya. Seperti yang disebutkan oleh Susanto et al., (2023), perkembangan teknologi informasi dan komunikasi telah memberikan banyak manfaat, namun di sisi lain juga menimbulkan risiko keamanan data, termasuk pencurian, manipulasi, dan peretasan sistem. Oleh karena itu, dengan menerapkan beberapa lapisan keamanan, termasuk deteksi situs terblokir, pemutusan jaringan otomatis, serta notifikasi *real-time*, sistem keamanan dapat lebih efektif dalam mengatasi ancaman.

Keuntungan utama dari strategi ini adalah keberlanjutan yang dimilikinya, di mana jika salah satu lapisan keamanan gagal, lapisan lainnya akan mengambil alih untuk mencegah ancaman tersebut. Hal ini sejalan dengan pandangan Aulia et al., (2023), yang menjelaskan bahwa jaringan komputer dan basis data memainkan peran vital dalam menjaga integritas sistem, di mana keamanan yang berlapis mampu mengelola infrastruktur yang terhubung secara global dengan lebih baik. Dengan demikian, keamanan berlapis memberikan fleksibilitas bagi *administrator* jaringan untuk memastikan bahwa kebijakan keamanan tetap terjaga meskipun ancaman semakin berkembang.

Dengan adanya tantangan keamanan siber yang semakin kompleks, pentingnya pengembangan sistem keamanan berlapis tidak dapat diabaikan. Hal ini

menekankan perlunya penerapan berbagai lapisan perlindungan untuk melindungi aset informasi. Konsep ini mengakui bahwa tidak ada satu mekanisme keamanan yang dapat memberikan perlindungan sempurna, sehingga kombinasi dari beberapa lapisan keamanan dapat menghasilkan perlindungan yang lebih baik. Melibatkan unsur teknologi, kebijakan, dan kesadaran pengguna menjadikan hal ini sebagai dasar yang kokoh untuk strategi keamanan informasi yang menyeluruh. Dengan implementasi keamanan berlapis, organisasi dapat meningkatkan ketahanan mereka terhadap serangan siber yang semakin kompleks dan canggih (Hoshmand & Ratnawati, 2023).

Pertama, lapisan deteksi situs terblokir berfungsi sebagai pertahanan awal. Sistem dapat secara efektif mengidentifikasi dan mencatat setiap upaya akses yang dilakukan oleh pengguna terhadap situs yang dikategorikan sebagai berbahaya atau melanggar kebijakan organisasi atau institusi pendidikan. Implementasi komponen ini dilakukan melalui *filter rules* dan *Layer 7 protocol* pada perangkat Mikrotik, yang memungkinkan sistem untuk secara aktif mendeteksi akses tidak sah.

Kedua, sebagai respon terhadap deteksi tersebut, sistem dilengkapi dengan mekanisme pemutusan jaringan otomatis yang berfungsi sebagai lapisan respon. Ketika pengguna terdeteksi mengakses situs terblokir, koneksi jaringan mereka akan secara otomatis diputus untuk jangka waktu tertentu, misalnya 30 menit. Langkah ini bertujuan sebagai tindakan pencegahan untuk mengatasi potensi pelanggaran kebijakan dan ancaman keamanan informasi.

Ketiga, lapisan *Monitoring* dilengkapi dengan sistem notifikasi berbasis Whatsapp yang memberikan pemberitahuan secara *real-time* kepada *administrator* jaringan setiap kali ada akses ke situs terblokir atau ketika pemutusan jaringan

dilakukan. Dengan fitur ini, *administrator* dapat dengan cepat merespons insiden keamanan dan melakukan *monitoring* yang lebih efektif.

Whatsapp adalah salah satu aplikasi mobile yang paling populer dan paling banyak digunakan. Aplikasi ini memungkinkan pengiriman pesan secara instan dan *real-time*, memberikan kemudahan dalam komunikasi serta meningkatkan efisiensi pengawasan jaringan (Purnama et al., 2023). Pemilihan Whatsapp sebagai platform notifikasi didasarkan pada penggunaannya yang meluas, aksesibilitas yang mudah, serta kemampuannya untuk mengirim pesan dengan cepat. Menurut *We Are Social & Meltwater* (2023), sekitar 92,1% pengguna internet di Indonesia menggunakan Whatsapp, menjadikannya aplikasi pesan instan paling banyak digunakan. Whatsapp memungkinkan *administrator* jaringan untuk menerima notifikasi di mana saja secara *real-time*, tanpa terikat pada aplikasi khusus atau perangkat tertentu. Dengan dukungan API yang mudah diintegrasikan, Whatsapp menjadi pilihan ideal untuk sistem notifikasi dalam pengelolaan keamanan jaringan.

Pemanfaatan Whatsapp sebagai platform notifikasi memberikan banyak keuntungan, seperti kemudahan penggunaan, kecepatan respons, dan familiaritas di kalangan pengguna. *administrator* jaringan dapat menerima notifikasi langsung melalui perangkat seluler, sehingga meningkatkan fleksibilitas dan efektivitas dalam memonitor sistem keamanan. Dengan integrasi ini, *Monitoring* keamanan jaringan dapat dilakukan secara lebih efisien dan *real-time*, terutama di lingkungan yang membutuhkan respon cepat terhadap potensi pelanggaran keamanan.

Keberhasilan sistem ini juga sangat bergantung pada perangkat jaringan yang digunakan, salah satunya adalah Mikrotik. Mikrotik merupakan perangkat jaringan yang populer di kalangan institusi pendidikan dan bisnis, karena

fleksibilitasnya dalam mengelola lalu lintas jaringan dan keamanan. Perangkat ini menawarkan fitur-fitur yang diperlukan untuk mengimplementasikan keamanan berlapis, seperti *Firewall*, pemfilteran konten, dan manajemen bandwidth yang memungkinkan *administrator* jaringan untuk dengan mudah mengontrol akses pengguna terhadap situs-situs tertentu. Penelitian-penelitian terdahulu memberikan gambaran dasar mengenai kemampuan Mikrotik dalam meningkatkan keamanan jaringan, seperti yang dijelaskan oleh Irawan et al., (2018). Penelitian yang dilakukan oleh Irawan et al., (2018) menunjukkan efektivitas penggunaan Mikrotik *RouterOS* dalam implementasi keamanan jaringan. Terlepas dari berbagai fitur keamanan bawaan yang sudah ada, masih ada ruang untuk pengembangan sistem keamanan yang lebih canggih dan terintegrasi.

Salah satu tantangan utama dalam pengelolaan keamanan jaringan adalah kontrol akses terhadap situs-situs yang dianggap berbahaya atau tidak sesuai dengan kebijakan organisasi. Pemblokiran situs-situs tertentu telah menjadi praktik umum di berbagai sektor, termasuk pendidikan. Namun, pemblokiran saja tidak selalu efektif dalam mengatasi tantangan keamanan, terutama dengan adanya teknologi yang memungkinkan *bypass* terhadap pemblokiran tersebut. Di SMKN 1 Arosbaya, sebuah sekolah kejuruan di Indonesia dengan program keahlian Teknik komputer dan Jaringan (TKJ), tantangan serupa muncul. Meskipun pemblokiran situs sudah diterapkan, kesulitan dalam mendeteksi akses ilegal secara *real-time* masih menjadi masalah yang dihadapi.

Dalam wawancara dengan Bapak Badrus Sulaiman, S.Pd., selaku Kepala Kompetensi Keahlian (Kakomli) TKJ sekaligus pengelola jaringan komputer di SMKN 1 Arosbaya pada tanggal 14 Oktober 2024, dijelaskan bahwa pemblokiran

situs di sekolah sepenuhnya bergantung pada kebijakan dari Kominfo, yang diimplementasikan oleh *Internet Service Provider(ISP)* yang digunakan. Hal ini berarti bahwa situs-situs terlarang hanya diblokir jika sudah masuk dalam daftar pemblokiran nasional. Namun, kelemahan dari sistem ini adalah siswa masih bisa mengakses situs terlarang menggunakan aplikasi pihak ketiga, seperti VPN, yang dapat menyamarkan aktivitas mereka. Bapak Badrus menegaskan bahwa situasi ini berada di luar kendali pihak sekolah dan menimbulkan tantangan serius dalam pengelolaan keamanan jaringan. Oleh karena itu, diperlukan solusi tambahan yang dapat memantau dan merespons secara lebih aktif terhadap upaya *bypass* yang mungkin dilakukan oleh siswa.

Solusi berbasis Whatsapp untuk notifikasi *real-time* terkait akses ke situs terblokir dianggap sebagai langkah yang relevan dan praktis, terutama karena Whatsapp sudah digunakan secara luas oleh *administrator* jaringan sekolah. Penelitian ini bertujuan mengembangkan sistem keamanan berlapis yang dapat mendeteksi akses ke situs terblokir dan secara otomatis memutuskan koneksi jaringan pada perangkat Mikrotik. Selain itu, sistem ini juga akan memberikan notifikasi langsung melalui Whatsapp sebagai bentuk *monitoring*. Dengan adanya tiga lapisan perlindungan ini deteksi, pemutusan otomatis, dan notifikasi *real-time* diharapkan dapat meningkatkan efektivitas dan efisiensi dalam pengelolaan keamanan jaringan di lingkungan pendidikan seperti SMKN 1 Arosbaya, sekaligus meminimalisir risiko akses yang tidak diinginkan.

Beberapa penelitian terdahulu telah membahas aspek-aspek yang relevan dengan pengembangan sistem keamanan berlapis berbasis Whatsapp untuk deteksi situs terblokir dan pemutusan jaringan otomatis pada Mikrotik. Beberapa studi

tersebut memberikan dasar yang kuat untuk penelitian ini, meskipun belum mengintegrasikan berbagai komponen keamanan seperti yang diusulkan dalam penelitian ini. Berikut adalah tinjauan dari beberapa penelitian tersebut:

Irawan et al., (2018) mengkaji penggunaan Mikrotik *RouterOS* untuk meningkatkan keamanan jaringan. Penelitian ini fokus pada implementasi fitur-fitur keamanan bawaan Mikrotik seperti *Firewall*, web proxy, dan manajemen bandwidth. Hasil penelitian menunjukkan bahwa implementasi sistem keamanan menggunakan Mikrotik *RouterOS* berhasil meningkatkan keamanan dan kinerja jaringan secara signifikan. Penelitian Irawan et al., (2018) memberikan dasar yang kuat untuk penggunaan Mikrotik sebagai platform utama dalam implementasi sistem keamanan jaringan. Namun, penelitian tersebut belum membahas aspek deteksi situs terblokir dan pemutusan jaringan otomatis yang menjadi fokus dalam penelitian ini.

Rasmin et al., (2024) mengkaji penggunaan Whatsapp API untuk meningkatkan efektivitas administrasi kepegawaian melalui notifikasi *real-time*. Penelitian ini fokus pada integrasi sistem berbasis website yang memungkinkan notifikasi otomatis dikirimkan kepada pengguna yang mengajukan izin atau cuti, serta kepada pihak yang bertanggung jawab untuk memverifikasi pengajuan tersebut. Hasil penelitian menunjukkan bahwa sistem ini mampu mempercepat proses administrasi dan memberikan notifikasi secara efisien kepada pihak terkait. Meskipun konteksnya berbeda, penelitian (Rasmin et al., 2024) mendemonstrasikan efektivitas penggunaan Whatsapp sebagai platform notifikasi dalam sistem *Monitoring* otomatis. Pendekatan ini dapat diadaptasi untuk sistem notifikasi dalam konteks keamanan jaringan.

Aziz et al., (2024) mengkaji penggunaan *Firewall filter rules* pada Mikrotik untuk meningkatkan keamanan jaringan. Penelitian ini fokus pada konfigurasi aturan *Firewall* untuk memblokir akses ke situs-situs tertentu dan mencegah serangan DoS. Penelitian (Aziz et al., 2024) memberikan pemahaman mendalam tentang penggunaan *Firewall filter rules* pada Mikrotik, yang merupakan komponen penting dalam implementasi deteksi situs terblokir pada penelitian ini.

Purnama et al., (2023) mengkaji penggunaan Snort IDS untuk mendeteksi serangan jaringan dan mengirimkan notifikasi *real-time* melalui Whatsapp dan Telegram. Penelitian ini berhasil mengintegrasikan sistem deteksi intrusi dengan layanan pesan instan untuk memberikan notifikasi ketika terjadi serangan, seperti ping attack, *port scanning*, dan DDoS. Namun, penelitian ini lebih berfokus pada deteksi serangan jaringan secara umum daripada deteksi akses ke situs terblokir dan pemutusan koneksi jaringan

Berdasarkan tinjauan terhadap penelitian-penelitian terdahulu, terdapat beberapa gap yang menjadi fokus penelitian ini. Pertama, meskipun beberapa penelitian telah membahas implementasi pemblokiran situs menggunakan Mikrotik, belum ada yang secara spesifik mengintegrasikan deteksi akses ke situs terblokir dengan mekanisme pemutusan jaringan otomatis. Oleh karena itu, penelitian ini bertujuan untuk mengembangkan sistem yang tidak hanya memblokir akses ke situs tertentu, tetapi juga secara otomatis memutus koneksi pengguna yang mencoba mengakses situs tersebut. Kedua, penggunaan Whatsapp sebagai platform notifikasi dalam konteks keamanan jaringan masih relatif baru, meskipun Whatsapp telah terbukti efektif sebagai platform notifikasi di berbagai konteks lainnya. Penelitian ini berupaya mengintegrasikan Whatsapp ke dalam sistem keamanan

jaringan untuk memberikan metode notifikasi yang lebih efisien dan *real-time* kepada *administrator* terkait insiden keamanan. Ketiga, meskipun banyak penelitian telah membahas fitur keamanan pada Mikrotik, pendekatan keamanan berlapis yang mengintegrasikan deteksi, respons, dan *Monitoring* dalam satu sistem belum banyak dieksplorasi. Penelitian ini berusaha mengembangkan sistem keamanan berlapis yang memanfaatkan kemampuan Mikrotik dan menambahkan fungsionalitas baru. Selain itu, kebanyakan penelitian terdahulu hanya berfokus pada implementasi teknis dari fitur keamanan tertentu, sementara penelitian ini tidak hanya mengimplementasikan sistem keamanan berlapis, tetapi juga mengevaluasi efektivitasnya dalam meningkatkan keamanan jaringan secara keseluruhan.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, maka rumusan masalah dalam penelitian ini adalah:

1. Bagaimana mekanisme keamanan berlapis berbasis Whatsapp dapat mendeteksi percobaan akses ke situs terblokir pada jaringan Mikrotik?
2. Bagaimana menerapkan mekanisme pemutusan jaringan otomatis pada perangkat Mikrotik ketika pengguna mencoba mengakses situs terblokir?
3. Bagaimana integrasi notifikasi berbasis Whatsapp dapat membantu *administrator* jaringan dalam melakukan pemantauan dan respon cepat terhadap ancaman keamanan?

1.3 Tujuan Penelitian Pengembangan

Berdasarkan permasalahan yang dirumuskan, tujuan penelitian ini yaitu :

1. Mengembangkan mekanisme keamanan berlapis berbasis Mikrotik yang dapat mendeteksi akses ke situs terblokir secara *real-time*
2. Menerapkan mekanisme pemutusan jaringan otomatis pada perangkat Mikrotik ketika mendeteksi akses ke situs terblokir
3. Mengintegrasikan sistem notifikasi Whatsapp untuk memberikan informasi *real-time* kepada *administrator* jaringan mengenai upaya akses situs terblokir dan pemutusan koneksi

1.4 Spesifikasi Produk Yang Diharapkan

Spesifikasi produk yang diharapkan dari penelitian ini mencakup pengembangan sebuah sistem keamanan jaringan yang meliputi:

1. Deteksi Situs Terblokir: Sistem harus mampu mendeteksi upaya akses ke situs yang telah dikategorikan sebagai terblokir atau berbahaya, menggunakan *filter rules* dan protokol Layer 7 pada Mikrotik.
2. Pemutusan Jaringan Otomatis: Sistem harus dapat secara otomatis memutus koneksi jaringan pengguna yang mencoba mengakses situs terblokir, dengan durasi pemutusan yang dapat dikonfigurasi (misalnya, 30 menit).
3. Notifikasi Whatsapp: Sistem harus mengirimkan notifikasi *real-time* melalui Whatsapp kepada *administrator* jaringan setiap kali terjadi upaya akses ke situs terblokir dan pemutusan jaringan.

1.5 Batasan Penelitian Pengembangan

Meskipun penelitian ini menawarkan potensi yang besar untuk meningkatkan keamanan jaringan, terdapat beberapa tantangan dan batasan yang perlu diperhatikan:

1. Keterbatasan Platform

Penelitian ini fokus pada implementasi sistem keamanan berlapis pada platform Mikrotik. Meskipun Mikrotik banyak digunakan, terutama di institusi pendidikan, hasil penelitian mungkin tidak dapat langsung diterapkan pada platform *networking* lainnya tanpa modifikasi.

2. Dinamika Ancaman Keamanan

Ancaman keamanan siber terus berkembang dengan cepat. Sistem yang dikembangkan dalam penelitian ini perlu dirancang dengan fleksibilitas yang cukup untuk dapat beradaptasi dengan ancaman baru yang mungkin muncul di masa depan.

3. Privasi dan Etika

Implementasi mekanisme keamanan yang melibatkan *Monitoring* aktivitas pengguna dan pemutusan jaringan otomatis memunculkan pertanyaan etis terkait privasi dan hak pengguna. Penelitian ini perlu mempertimbangkan dan mengelola aspek-aspek etis ini dengan hati-hati.

4. Ketergantungan pada Layanan Pihak Ketiga

Penggunaan Whatsapp sebagai platform notifikasi menciptakan ketergantungan pada layanan pihak ketiga. Perlu dipertimbangkan rencana pengganti jika terjadi gangguan pada layanan Whatsapp.

5. Skalabilitas

Meskipun penelitian ini bertujuan untuk mengembangkan sistem yang dapat diimplementasikan oleh berbagai organisasi atau institusi, perlu diuji lebih lanjut bagaimana sistem ini berperforma dalam skala yang lebih besar atau dalam lingkungan jaringan yang lebih kompleks.

6. Kepatuhan Regulasi

Implementasi sistem keamanan jaringan perlu mempertimbangkan aspek kepatuhan terhadap regulasi yang berlaku, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia. Penelitian ini perlu memastikan bahwa sistem yang dikembangkan sejalan dengan kerangka hukum yang berlaku.

1.6 Pentingnya Penelitian Pengembangan

Penelitian ini penting karena:

1. Meningkatkan Keamanan Jaringan: Mengembangkan mekanisme keamanan berlapis yang lebih canggih dapat membantu institusi pendidikan dan organisasi dalam melindungi infrastruktur teknologi mereka dari ancaman siber.
2. Menjawab Kebutuhan Pengelolaan Jaringan yang Lebih Efektif: Dalam era digital, pengelolaan jaringan yang lebih aktif dan responsif terhadap ancaman adalah suatu keharusan. Mekanisme keamanan yang dikembangkan dalam penelitian ini dapat memberikan solusi yang lebih efisien dalam pengelolaan akses internet.
3. Kontribusi pada Sistem Keamanan Berbasis Whatsapp: Penelitian ini memberikan kontribusi inovatif dengan mengintegrasikan Whatsapp sebagai platform notifikasi *real-time* dalam sistem keamanan jaringan, yang masih relatif jarang dilakukan.
4. Pengembangan Model Keamanan yang Dapat Diadaptasi: Mekanisme keamanan ini dapat menjadi model yang dapat diadaptasi oleh berbagai

organisasi dan institusi pendidikan lain untuk meningkatkan keamanan jaringan mereka.

1.7 Definisi Istilah

Definisi istilah yang terdapat dalam penelitian ini adalah :

1. Mikrotik: Perangkat jaringan yang digunakan untuk mengelola sistem jaringan, termasuk *Firewall* , pemfilteran konten, dan manajemen bandwidth.
2. Whatsapp API: Antarmuka pemrograman aplikasi yang memungkinkan integrasi aplikasi pihak ketiga dengan layanan pesan Whatsapp untuk mengirim notifikasi otomatis.
3. *Layer 7 Protocol*: Protokol yang berfungsi pada lapisan aplikasi dalam model *OSI*, sering digunakan untuk *filter* konten web dan deteksi aplikasi di jaringan.
4. Pemutusan Jaringan Otomatis: Mekanisme yang secara otomatis memutuskan koneksi jaringan pengguna ketika mendeteksi akses ke situs yang terblokir atau tidak sesuai kebijakan.
5. Notifikasi *Real-time*: Pemberitahuan yang dikirimkan secara instan kepada *administrator* jaringan mengenai aktivitas tertentu, seperti upaya akses ke situs terblokir.
6. *Defense in Depth* (Keamanan Berlapis): Strategi keamanan yang menggunakan beberapa lapisan perlindungan untuk mengamankan sistem atau aset informasi.