

BAB I

PENDAHULUAN

1.1 Latar Belakang

Ancaman siber di Indonesia saat ini menunjukkan skala yang besar dan jenisnya semakin banyak. Berdasarkan laporan (Badan Siber dan Sandi Negara (BSSN), 2024), tercatat sebanyak 330.527.636 trafik anomali serangan siber selama tahun berjalan, yang meliputi aktivitas botnet, ransomware, dan phishing. Aktivitas botnet Mirai menjadi yang terbesar dengan lebih dari 81 juta serangan, disusul 514 ribu serangan ransomware yang berpotensi melumpuhkan layanan publik, serta 5.780 kasus web defacement yang banyak menargetkan situs pemerintah dan lembaga pendidikan. Kondisi tersebut menunjukkan bahwa sektor publik, termasuk sekolah dan universitas, sangat rentan terhadap serangan siber. Jumlah 1.814 laporan serangan siber menjadi bukti rendahnya kesiapan organisasi dalam merespons ancaman digital. Hal ini menegaskan bahwa ancaman siber di Indonesia bukan lagi masalah teknis, melainkan tantangan strategis nasional. Karena itu, diperlukan langkah mitigasi berlapis, terutama pada sektor pendidikan yang masih minim perlindungan infrastruktur digital.

Selain jumlah serangan yang meningkat, kompleksitas ancaman siber di Indonesia juga semakin tinggi karena melibatkan kelompok kriminal terorganisir. Berdasarkan Laporan (SOCRadar, 2025), menunjukkan bahwa sektor pendidikan menjadi target ancaman terbesar kedua di dark web dengan porsi 12,59%, setelah sektor keuangan. Sebanyak 88,12% ancaman berupa kebocoran data dan 28,8% serangan ransomware secara khusus menarget Indonesia, menunjukkan daya tarik ekonomi bagi pelaku kejahatan siber. Dampaknya tidak hanya menimbulkan

kerugian finansial, tetapi juga menurunkan kepercayaan masyarakat terhadap layanan digital. Kondisi ini diperburuk oleh maraknya phishing dan scam yang menasar sektor pendidikan. Dengan demikian, lembaga pendidikan kini menjadi salah satu sasaran utama yang harus dilindungi secara serius. Oleh karena itu, diperlukan arsitektur keamanan jaringan yang komprehensif untuk memastikan deteksi dini, pencegahan, dan respons cepat guna menjaga keberlangsungan pembelajaran digital serta melindungi data akademik.

Banyak sekolah di Indonesia mengandalkan teknologi digital, namun infrastruktur jaringannya masih minim standar keamanan. Router, server, dan Wi-Fi biasanya hanya mendukung konektivitas tanpa konfigurasi proteksi, sehingga mudah diserang malware, port scanning, atau akses ilegal. Menurut penelitian (Zulfikri et al., 2023), jaringan tanpa *firewall* dan port blocking lebih rentan terhadap serangan eksternal. Keterbatasan tenaga ahli dan pemantauan yang minim membuat serangan ringan pun sering tidak terdeteksi. Hal ini menunjukkan bahwa infrastruktur jaringan sekolah masih sangat rawan terhadap ancaman siber.

Selain kerentanan jaringan, kebocoran data akademik juga menjadi masalah serius di sekolah. Data siswa, guru, dan catatan akademik sering tersimpan di server tanpa perlindungan enkripsi maupun kontrol akses berlapis. Kondisi ini membuat data mudah dicuri atau disalahgunakan melalui malware, Trojan, atau ransomware. Menurut Penelitian (Nadira, 2024), ransomware mendominasi hingga 82,78% dari insiden serangan yang terdeteksi di Indonesia. Tingginya angka ini menunjukkan bahwa kebocoran data bukan lagi ancaman potensial, tetapi masalah nyata yang terus meningkat. Apabila terjadi kebocoran, sekolah dapat mengalami penyalahgunaan identitas dan terganggunya proses administrasi.

Situasi ini menegaskan bahwa proteksi data akademik seharusnya menjadi prioritas utama lembaga pendidikan.

Rendahnya kesadaran terhadap ancaman siber di lingkungan pendidikan membuat siswa dan guru rentan terhadap serangan seperti phishing, situs palsu, dan tautan berbahaya. Kondisi ini meningkatkan risiko kebocoran data serta gangguan pada proses pembelajaran. Menurut Penelitian (Maulidi, 2024), menunjukkan bahwa tingkat kesadaran keamanan siber di kalangan pelajar SMP masih rendah, sehingga serangan sering tidak terdeteksi sejak dini. Kurangnya pemahaman dasar juga membuat informasi sensitif lebih mudah bocor dan upaya pencegahan di tingkat pengguna kurang efektif. Hal ini menegaskan bahwa faktor manusia menjadi titik rawan dalam keamanan jaringan sekolah.

Fenomena rendahnya kesadaran terhadap keamanan siber tersebut juga ditemukan di lingkungan MA Manbaul Ulum, yang telah memanfaatkan jaringan internet dalam berbagai aktivitas pembelajaran dan administrasi sekolah. Berdasarkan hasil observasi, di sekolah ini telah menggunakan layanan IndiBiz dengan kecepatan hingga 150 Mbps serta didukung perangkat router, switch, dan *access point* di setiap ruang kelas. Meskipun secara infrastruktur sudah tergolong memadai, namun belum dilengkapi dengan sistem keamanan yang terintegrasi untuk mendeteksi dan mencegah ancaman siber secara dini. Pengelolaan jaringan masih dilakukan secara manual oleh administrator tanpa *monitoring* otomatis. Akibatnya, gangguan atau serangan baru baru terdeteksi setelah adanya laporan pengguna. Kondisi ini menunjukkan bahwa selain faktor manusia, aspek teknis dan manajerial juga menjadi titik lemah dalam keamanan jaringan sekolah. Oleh karena itu, diperlukan penerapan sistem keamanan terintegrasi yang dapat

memantau jaringan secara *real-time*, mencatat aktivitas melalui log otomatis, dan memberikan notifikasi dini terhadap potensi ancaman.

Selain masalah konektivitas, aspek keamanan jaringan di MA Manbaul Ulum masih sangat terbatas. Sekolah belum menerapkan *firewall* seperti IPTables, sehingga perlindungan terhadap ancaman eksternal belum memadai. *Monitoring* jaringan masih dilakukan secara manual tanpa dukungan sistem seperti Zabbix untuk peringatan dini. Berdasarkan hasil wawancara dengan Bapak Muhammad Minan Nur Rohman, selaku Guru Informatika sekaligus Administrator Jaringan, pada hari Sabtu, 23 Agustus 2025 pukul 10.00, diperoleh informasi bahwa pernah terjadi insiden serangan siber berupa file PDF berbahaya yang membuat komputer guru freeze dan tidak responsif. Penanganan insiden masih bersifat reaktif melalui instal ulang dan pemulihan data, sementara langkah pencegahan hanya berupa imbauan kepada guru dan siswa. Oleh karena itu, penerapan sistem keamanan jaringan yang terstruktur, proaktif, dan terintegrasi menjadi kebutuhan mendesak untuk menjaga proses pembelajaran berbasis digital.

Berdasarkan permasalahan di MA Manbaul Ulum, sekolah memerlukan sistem keamanan jaringan yang tidak hanya menyediakan akses internet, tetapi juga mengintegrasikan *monitoring* dan pengelolaan status paket secara *real-time*. Sistem *monitoring* dibutuhkan untuk mendeteksi ancaman lebih cepat tanpa menunggu laporan manual dari pengguna. Penerapan *firewall* stateful seperti IPTables dapat memberikan perlindungan tambahan dengan memeriksa setiap paket data masuk dan keluar. *Firewall* juga mencatat status koneksi sehingga ancaman seperti virus, malware, dan akses ilegal dapat dicegah sejak dini. Integrasi kedua aspek ini membuat pengelolaan jaringan lebih efisien, aman, dan

mendukung kelancaran pembelajaran digital. Dengan sistem keamanan terstruktur dan terintegrasi, MA Manbaul Ulum diharapkan meningkatkan kualitas layanan TI sekaligus menjaga jaringan tetap stabil, andal, dan terlindungi dari serangan siber.

Salah satu solusi utama untuk meningkatkan keamanan jaringan sekolah adalah menerapkan Zabbix sebagai sistem *monitoring real-time*. Zabbix mampu mengawasi perangkat jaringan, beban server, dan lalu lintas data, serta memberikan notifikasi melalui Telegram saat terjadi anomali (Heti et al., 2024). Kemampuan ini memungkinkan deteksi insiden lebih cepat sehingga serangan dapat diminimalkan sebelum berdampak luas. Penggunaan Linux Ubuntu Server sebagai basis Zabbix membuat sistem lebih ringan, fleksibel, dan cocok untuk perangkat dengan spesifikasi terbatas. Fitur network mapping membantu administrator memahami topologi jaringan dan titik rawan yang perlu diawasi. Penelitian sebelumnya menunjukkan bahwa penerapan Zabbix mempercepat proses troubleshooting dibandingkan mengandalkan laporan manual, sehingga menjadi solusi strategis menghadapi ancaman digital.

Penerapan Zabbix di SMK Negeri 4 Kota Bengkulu menunjukkan bahwa sistem *monitoring* jaringan berbasis open source ini efektif mendukung kegiatan pendidikan (Julian et al., 2022). Zabbix memungkinkan administrator memantau status host, router, dan perangkat lain serta menampilkan laporan performa dalam bentuk grafik yang mudah dipahami. Sistem ini dapat diakses melalui web browser, sehingga fleksibel digunakan dari berbagai perangkat. Hasil pengujian menunjukkan bahwa troubleshooting jaringan menjadi lebih cepat dan efisien setelah penerapan Zabbix. Dengan metode *Network Development Life Cycle*

(NDLC), implementasi dilakukan secara terstruktur dari analisis kebutuhan hingga manajemen berkelanjutan, membuktikan bahwa Zabbix meningkatkan efisiensi teknis sekaligus mendukung kelancaran pembelajaran digital. Selain *monitoring*, aspek pencegahan juga penting dilakukan dengan menerapkan kebijakan *firewall* berbasis IPTables. *Firewall* bertugas membatasi akses lalu lintas data, memfilter paket berbahaya, dan mencegah serangan umum seperti *port scanning*, *SYN flood*, maupun akses ilegal (Budi & Sembiring, 2025). Dengan mekanisme *stateful packet filtering*, IPTables mampu menyimpan informasi koneksi aktif, sehingga hanya lalu lintas sah yang dapat melewati jaringan internal.

Penerapan *firewall* memungkinkan pembentukan (*Demilitarized Zone*) DMZ untuk memisahkan layanan publik seperti web server dari jaringan internal, sehingga keamanan lebih terjamin. Pengujian menunjukkan bahwa IPTables berhasil memblokir berbagai serangan simulasi, seperti *NULL attack* dan *XMAS attack*, serta mencatat aktivitas mencurigakan ke log sistem. Integrasi *firewall* penting karena jaringan sekolah digunakan secara bebas oleh guru dan siswa. Dengan kombinasi Zabbix sebagai sistem *monitoring real-time* dan IPTables sebagai mekanisme pencegahan, sekolah dapat membangun arsitektur keamanan berlapis. Sistem ini mampu mendeteksi sekaligus menahan serangan siber secara efektif.

Meskipun IPTables dan Zabbix telah terbukti efektif dalam meningkatkan keamanan jaringan secara terpisah, penerapan integrasi keduanya di lingkungan sekolah masih jarang diteliti secara menyeluruh. Sebagian besar penelitian sebelumnya hanya berfokus pada aspek teknis, tanpa mempertimbangkan

penerapan yang selaras dengan kondisi nyata sekolah. Oleh karena itu, penelitian ini berjudul “Implementasi Arsitektur Keamanan Jaringan Sekolah Menggunakan Sistem *Monitoring Zabbix* dan *Firewall IPTables*” yang bertujuan untuk merancang dan mengkaji arsitektur keamanan jaringan terintegrasi berbasis iptables dan zabbix, sehingga mampu meningkatkan kemampuan deteksi, pencegahan, dan respons terhadap ancaman siber secara lebih efektif di lingkungan pendidikan.

1.2 Rumusan Masalah

Berdasarkan Latar Belakang dan masalah-masalah yang sudah dijelaskan, maka rumusan masalah pada penelitian ini yaitu :

1. Bagaimana implementasi sistem keamanan jaringan berbasis *Monitoring Zabbix* dan *Firewall IPTables* dalam meningkatkan deteksi dini dan pencegahan serangan di MA Manbaul Ulum?
2. Bagaimana hasil pengujian dan evaluasi kinerja sistem *Monitoring Zabbix* dengan berbantuan *IPTables* pada jaringan MA Manbaul Ulum berdasarkan standar ISO/IEC 27001:2022.

1.3 Tujuan Penelitian Pengembangan

Berdasarkan latar belakang dan rumusan masalah yang telah dijabarkan sebelumnya, tujuan dari penelitian ini adalah sebagai berikut:

1. Untuk mengimplementasikan, menguji, dan mengevaluasi kinerja sistem keamanan jaringan berbasis *Monitoring Zabbix* dan *Firewall IPTables* dalam meningkatkan deteksi ancaman, efektivitas pencegahan serangan, serta efisiensi proses *Troubleshooting* di MA Manbaul Ulum.

2. Untuk mengetahui dan mengevaluasi kinerja sistem *Monitoring Zabbix* dengan berbantuan *IPTables* pada jaringan MA Manbaul Ulum berdasarkan standar ISO/IEC 27001-2022.

1.4 Spesifikasi Produk yang Diharapkan

Spesifikasi produk sistem keamanan jaringan yang dikembangkan oleh peneliti diharapkan sebagai berikut:

1. Spesifikasi Perangkat Keras (Hardware)

Perangkat keras minimum yang dibutuhkan untuk menjalankan sistem *monitoring* dan *firewall* antara lain:

- a. Server atau PC dengan prosesor minimal Intel Core i3 atau setara.
- b. RAM minimal 4 GB, disarankan 8 GB untuk performa optimal.
- c. Storage minimal 100 GB, disarankan menggunakan SSD untuk kecepatan baca-tulis data.
- d. Koneksi jaringan LAN/Wi-Fi stabil untuk integrasi *monitoring* dan *firewall*.
- e. Router dan switch jaringan yang mendukung segmentasi dan manajemen lalu lintas.
- f. Sistem operasi Linux Debian/Ubuntu sebagai basis implementasi *IPTables* dan *Zabbix*.

2. Spesifikasi Perangkat Lunak (Software)

Aplikasi atau sistem yang digunakan memiliki spesifikasi sebagai berikut:

- a. *Zabbix* Server versi 6.0 LTS atau yang lebih baru.
- b. *Firewall* *IPTables* berbasis Linux dengan konfigurasi rules sesuai kebutuhan keamanan jaringan sekolah.
- c. Bot WhatsApp bot untuk notifikasi *real-time* dari *Zabbix*.

- d. Web browser untuk mengakses antarmuka Zabbix (Chrome, Firefox, dsb).

3. Spesifikasi Fitur Sistem

Fitur-fitur yang dikembangkan dalam sistem keamanan jaringan meliputi:

a. *Monitoring Jaringan Real-Time*

Menampilkan status perangkat jaringan, trafik data, dan beban server melalui antarmuka web.

b. Peringatan dan Notifikasi

Mengirimkan alert otomatis melalui Whatsapp saat terjadi gangguan atau anomali jaringan.

c. Konfigurasi *Firewall* IPTables

Melindungi jaringan dari akses tidak sah, menyaring lalu lintas, dan membatasi akses layanan berdasarkan IP, port, atau protokol tertentu.

d. Histori dan Log Pemantauan

Penyimpanan data historis untuk audit, evaluasi, dan analisis jaringan secara berkala.

4. Target Pengguna Sistem

Target pengguna dari sistem keamanan jaringan ini adalah:

- a. Administrator jaringan sekolah yang bertugas mengelola infrastruktur TI.
- b. Tim teknis sekolah yang bertanggung jawab atas keamanan dan kestabilan jaringan.
- c. Staf IT MA yang membutuhkan sistem keamanan ringan, terintegrasi, dan mudah dipelajari. Sistem ini juga dapat dijadikan acuan atau template bagi sekolah lain dengan kebutuhan serupa dalam membangun arsitektur keamanan jaringan yang efisien.

1.5 Batasan Penelitian Pengembangan

Agar penelitian ini terfokus dan dapat dilaksanakan secara efektif sesuai dengan sumber daya yang tersedia, maka batasan penelitian pengembangan ini ditetapkan sebagai berikut:

1. Lingkup Implementasi

Penelitian ini hanya dilakukan di lingkungan jaringan sekolah MA Manbaul Ulum sebagai objek penelitian, dan tidak mencakup implementasi di seluruh sekolah atau institusi lain secara langsung. Uji coba sistem dilakukan pada jaringan lokal (LAN) atau jaringan nirkabel (Wi-Fi) yang terhubung dengan infrastruktur sekolah.

2. Cakupan Sistem *Monitoring*

Sistem *monitoring* yang digunakan terbatas pada Zabbix versi 6.0 LTS (atau versi setara) untuk memantau perangkat dan layanan jaringan secara *real-time*.

3. Cakupan *Firewall*

Firewall yang digunakan adalah IPTables berbasis sistem operasi Linux Debian/Ubuntu. Penelitian tidak membahas konfigurasi *firewall* komersial atau perangkat keras khusus (*hardware firewall*) seperti Fortigate, Cisco ASA, atau Mikrotik.

4. Integrasi Sistem

Integrasi yang dibangun terbatas pada penghubungan Zabbix dengan IPTables dalam arsitektur keamanan jaringan. Integrasi tambahan seperti SIEM (*Security Information and Event Management*) atau IDS/IPS berbasis Suricata/Snort tidak dibahas secara mendalam.

5. Skalabilitas Sistem

Penelitian ini difokuskan pada skala jaringan sekolah dengan jumlah perangkat yang terbatas sesuai kondisi lapangan. Pengujian tidak mencakup skenario jaringan berskala besar seperti universitas atau data center.

6. Fokus Pengujian

Pengujian sistem berfokus pada aspek kemampuan deteksi gangguan dan efektivitas pencegahan akses ilegal melalui kombinasi *monitoring* Zabbix dan *firewall* IPTables. Aspek lain seperti performa server di bawah beban tinggi atau analisis keamanan tingkat lanjutan tidak menjadi fokus utama.

1.6 Pentingnya Penelitian Pengembangan

Penelitian pengembangan ini memiliki peran penting dalam upaya meningkatkan kualitas keamanan jaringan di lingkungan sekolah, khususnya di MA Manbaul Ulum. Seiring dengan meningkatnya ancaman siber, sekolah dituntut tidak hanya menyediakan layanan konektivitas, tetapi juga memastikan bahwa jaringan yang digunakan terlindungi dari potensi serangan. Implementasi sistem *monitoring* Zabbix dan *firewall* IPTables akan memberikan solusi komprehensif yang dapat memadukan deteksi dini dengan mekanisme pencegahan. Dengan adanya integrasi menyeluruh tersebut, administrator jaringan dapat lebih cepat mengidentifikasi gangguan, sekaligus mengambil langkah preventif agar serangan tidak berdampak luas.

Selain itu, penelitian ini juga penting karena dapat dijadikan referensi praktis bagi sekolah lain yang menghadapi kendala serupa dalam aspek keamanan jaringan. Produk penelitian berupa arsitektur keamanan berlapis akan memberikan kontribusi nyata dalam mendukung kelancaran pembelajaran digital, menjaga

integritas data akademik, serta meningkatkan kesadaran akan pentingnya perlindungan sistem informasi di lembaga pendidikan. Lebih jauh, penelitian ini diharapkan dapat memperkaya khazanah keilmuan di bidang keamanan jaringan dengan memberikan bukti empiris mengenai efektivitas kombinasi Zabbix dan IPTables dalam skala jaringan sekolah.

1.7 Definisi Istilah

Untuk mempermudah pemahaman terhadap istilah yang digunakan dalam penelitian ini, berikut beberapa definisi operasional:

1. Keamanan Jaringan

Suatu upaya sistematis dalam melindungi infrastruktur jaringan komputer dari akses tidak sah, penyalahgunaan, atau serangan siber yang dapat mengganggu ketersediaan, integritas, dan kerahasiaan data.

2. Zabbix

Aplikasi *open-source* berbasis server-client yang berfungsi sebagai sistem *monitoring real-time*. Zabbix mampu memantau perangkat, layanan, dan lalu lintas jaringan, serta memberikan notifikasi otomatis kepada administrator ketika terjadi gangguan atau anomali.

3. IPTables

Sebuah *firewall* berbasis sistem operasi Linux yang berfungsi untuk memfilter, mengatur, dan mengendalikan lalu lintas data berdasarkan aturan tertentu. IPTables mendukung mekanisme serapan sehingga hanya koneksi sah yang dapat melewati jaringan internal.

4. *Firewall*

Sistem pengaman yang bertugas mengatur lalu lintas jaringan dengan cara mengizinkan atau menolak paket data berdasarkan aturan keamanan yang ditentukan. *Firewall* berfungsi sebagai lapisan pelindung utama antara jaringan internal dengan jaringan luar.

5. *Monitoring Jaringan*

Proses pengawasan secara berkelanjutan terhadap kondisi perangkat keras, perangkat lunak dan lalu lintas data pada jaringan komputer untuk mendeteksi permasalahan maupun ancaman secara cepat dan tepat.