Jurnal Pengembangan Sains dan Teknologi
Volume 1, Nomor 1, Januari 2025, p. 25-41
ISSN : 3090-2762 (*Print*) | 3089-9516 (*Online*)
DOI : 10.63866/jpst.v1i1.39

Analisis Keamanan Jaringan pada Sistem Kendali Jarak Jauh untuk Infrastruktur Kritis

Zumhur Alamin[1*], Muhammad Amirul Mu'min[1]

[1]Program Studi Ilmu Komputer, Universitas Muhammadiyah Bima

Email Koresponden: zumhur.alamin@gmail.com
(* : corresponding author)

Abstrak- Keamanan jaringan pada sistem kendali jarak jauh untuk infrastruktur kritis menjadi isu yang penting seiring dengan meningkatnya ancaman siber yang dapat mengganggu operasional. Penelitian ini bertujuan untuk menganalisis tingkat keamanan pada sistem kendali jarak jauh di berbagai fasilitas infrastruktur kritis, dengan fokus pada ancaman eksternal dan internal. Pendekatan yang digunakan dalam penelitian ini adalah studi kasus dengan mengamati tiga fasilitas yang berbeda, serta mengidentifikasi berbagai jenis serangan yang dapat mengakses dan merusak sistem kendali. Hasil penelitian menunjukkan bahwa fasilitas dengan kebijakan keamanan yang kuat dan teknologi mitigasi yang canggih, seperti pembaruan perangkat lunak rutin dan kontrol akses berbasis peran (RBAC), lebih mampu mengatasi ancaman seperti serangan DDoS, *phishing*, dan serangan *zero-day*. Sebaliknya, fasilitas yang memiliki kebijakan keamanan lemah menunjukkan kerentanannya terhadap ancaman tersebut. Penelitian ini memberikan kontribusi penting terhadap pengembangan pengetahuan di bidang keamanan siber untuk infrastruktur kritis, serta memberikan rekomendasi terkait penerapan kebijakan dan teknologi mitigasi yang lebih baik untuk meningkatkan ketahanan sistem kendali jarak jauh.

Kata Kunci: Keamanan Jaringan, Infrastruktur Kritis, Ancaman Siber, Proteksi Jaringan

Network Security Analysis of Remote Control System for Critical Infrastructure

Abstract- *Network security of remote control systems for critical infrastructure is becoming an important issue as cyber threats increase that can disrupt operations. This research aims to analyze the security level of remote control systems in various critical infrastructure facilities, focusing on external and internal threats. The approach used in this research is a case study by observing three different facilities, and identifying different types of attacks that can access and damage the control system. The results showed that facilities with strong security policies and advanced mitigation technologies, such as regular software updates and role-based access control, were better able to cope with threats such as DDoS attacks, phishing, and zero-day attacks. In contrast, facilities with weak security policies showed their vulnerability to such threats. This research makes an important contribution to the development of knowledge in the field of cybersecurity for critical infrastructure, and provides recommendations regarding the implementation of better mitigation policies and technologies to improve the resilience of remote control systems.*

Keywords: *Network Security, Critical Infrastructure, Cyber Threats, Network Protection*

Received	Revised	Published
17-09-2024	10-12-2024	19-01-2025

1. PENDAHULUAN

Keamanan jaringan pada sistem kendali jarak jauh untuk infrastruktur kritis menjadi semakin penting dalam era digital yang penuh tantangan. Infrastruktur kritis, seperti pembangkit listrik, sistem distribusi energi, dan fasilitas transportasi, memainkan peran penting dalam kehidupan sehari-hari. Sistem kendali jarak jauh memungkinkan pengelolaan infrastruktur tersebut secara lebih efisien dan fleksibel. Namun, dengan meningkatnya ketergantungan pada teknologi jaringan, muncul pula ancaman terhadap keamanan yang dapat merusak integritas dan ketersediaan infrastruktur tersebut [1], [2]. Dalam beberapa tahun terakhir, serangan terhadap sistem kendali jarak jauh telah menunjukkan peningkatan signifikan, yang memunculkan keprihatinan akan kerentanannya terhadap ancaman siber [3].

Topik ini penting untuk diteliti karena keberhasilan pengelolaan infrastruktur kritis sangat bergantung pada integritas sistem kendali yang digunakan. Potensi serangan seperti *malware*, *ransomware*, dan akses ilegal dapat merusak sistem kendali, yang berakibat fatal pada kestabilan dan kelangsungan hidup infrastruktur yang bersangkutan, sebagaimana dibuktikan oleh insiden seperti serangan *ransomware* pada Eksekutif Layanan Kesehatan Irlandia, yang mengganggu layanan medis vital[4]. Misalnya, serangan terhadap jaringan distribusi energi dapat menyebabkan pemadaman listrik massal atau gangguan pada pasokan energi yang memengaruhi sektor-sektor penting lainnya. Selain itu, ancaman terhadap sistem transportasi dapat mengganggu sistem logistik yang sangat vital bagi perekonomian [4], [5].

Penelitian menunjukkan bahwa sementara enkripsi dan otentikasi adalah dasar untuk mengamankan sistem kendali jarak jauh, ada kesenjangan yang signifikan dalam mengeksplorasi langkah-langkah keamanan canggih seperti deteksi intrusi berbasis kecerdasan buatan dan pengawasan real-time untuk melawan ancaman canggih [6], [7]. Misalnya, Algoritma Pertukaran Kunci Dinamis (DKEA) dan Algoritma Mitigasi Ancaman Adaptif (ATMA) telah menunjukkan harapan dalam meningkatkan keamanan melalui manajemen kunci dinamis dan respons adaptif terhadap ancaman cyber yang berkembang [7]. Selain itu, integrasi fitur biometrik dan teknologi blockchain dalam skema enkripsi dapat meningkatkan keamanan dalam aplikasi penginderaan jauh, menyoroti kebutuhan akan solusi komprehensif yang membahas aspek teknis dan prosedural keamanan [8]. Selain itu, kebijakan dan prosedur operasional sangat penting dalam mengurangi risiko, menunjukkan bahwa pendekatan multi-segi yang menggabungkan teknologi dan tata kelola sangat penting untuk keamanan yang efektif dalam sistem kendali jarak jauh [9].

Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis kelemahan dalam sistem kendali jarak jauh yang digunakan untuk infrastruktur kritis, khususnya dari sisi keamanan jaringan. Penelitian ini akan mengevaluasi keberadaan celah-celah keamanan yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab dan memberikan rekomendasi untuk perbaikan pengamanan. Penelitian ini juga bertujuan untuk mengembangkan pemahaman tentang pentingnya pengawasan sistem yang lebih baik dan penggunaan teknologi terbaru dalam pengamanan infrastruktur kritis.

Kontribusi utama penelitian ini terletak pada penguatan kebijakan keamanan jaringan dalam infrastruktur kritis, serta penyusunan strategi mitigasi berbasis teknologi canggih untuk meningkatkan ketahanan sistem kendali jarak jauh. Hasil penelitian ini diharapkan dapat menjadi referensi bagi pengelola infrastruktur kritis dalam merancang kebijakan keamanan yang lebih adaptif dan efektif guna menghadapi ancaman siber yang terus berkembang.

2. METODE PENELITIAN

2.1 Desain Penelitian

Penelitian ini menggunakan desain penelitian deskriptif kualitatif untuk menganalisis keamanan jaringan pada sistem kendali jarak jauh yang diterapkan pada infrastruktur kritis. Pendekatan deskriptif kualitatif dipilih karena penelitian ini bertujuan untuk menggali dan menjelaskan fenomena yang ada secara mendalam, tanpa menguji hipotesis atau hubungan antar variabel. Penelitian ini bertujuan untuk mendapatkan gambaran yang jelas mengenai kelemahan dan celah dalam sistem keamanan jaringan pada infrastruktur kritis, serta memahami faktor-faktor yang berkontribusi terhadap kerentanannya.

2.2 Karakteristik Subjek dan Sampel

Sampel dalam penelitian ini terdiri dari tiga fasilitas infrastruktur kritis yang menggunakan sistem kendali jarak jauh untuk mengelola operasional mereka, yaitu: Pembangkit listrik (PLTU), Stasiun distribusi energi, Sistem manajemen transportasi publik. Masing-masing fasilitas dipilih berdasarkan kriteria inklusi yaitu fasilitas yang menggunakan sistem kendali jarak jauh berbasis jaringan elektronik yang terkoneksi dengan berbagai sistem digital. Kriteria eksklusi meliputi fasilitas yang tidak menggunakan sistem kendali jarak jauh atau belum memiliki infrastruktur jaringan yang memadai untuk mendukung pengelolaan jarak jauh.

Jumlah subjek yang terlibat dalam penelitian ini adalah 15 orang, yang terdiri dari staf teknis dan ahli keamanan yang berperan dalam pengelolaan sistem kendali dan pengamanan jaringan. Pemilihan subjek dilakukan dengan menggunakan teknik purposive sampling, di mana peserta dipilih berdasarkan keterlibatannya langsung dalam pengelolaan dan pengamanan jaringan pada fasilitas yang diteliti.

Justifikasi pemilihan tiga fasilitas ini didasarkan pada keterwakilan sektor infrastruktur kritis yang memiliki tingkat ketergantungan tinggi terhadap sistem kendali jarak jauh. Selain itu, keterbatasan akses ke fasilitas lain menjadi kendala dalam memperluas cakupan penelitian, mengingat sensitivitas dan kebijakan keamanan yang berlaku di banyak sektor infrastruktur kritis. Dengan demikian, hasil penelitian ini dapat memberikan gambaran yang cukup representatif mengenai tantangan dan strategi pengamanan yang diterapkan dalam sistem kendali jarak jauh, meskipun cakupan fasilitas yang diteliti masih terbatas.

2.3 Instrumen Pengumpulan Data

Instrumen utama yang digunakan dalam penelitian ini adalah wawancara semi-terstruktur dan observasi lapangan. Wawancara dirancang untuk menggali informasi mendalam mengenai kebijakan pengamanan yang diterapkan, kesadaran akan potensi ancaman, serta kendala yang dihadapi dalam pengelolaan keamanan jaringan. Instrumen wawancara divalidasi oleh pakar di bidang keamanan siber dan infrastruktur kritis untuk memastikan bahwa pertanyaan yang diajukan relevan dan komprehensif. Selain itu, instrumen ini diuji reliabilitasnya melalui uji coba pada sejumlah kecil responden sebelum diterapkan pada sampel utama.

Observasi lapangan dilakukan untuk memeriksa langsung implementasi kebijakan pengamanan dan teknologi yang digunakan di setiap fasilitas, seperti perangkat keamanan yang dipasang, sistem pemantauan jaringan, serta prosedur yang diterapkan dalam pengawasan dan pengelolaan ancaman. Data dari observasi ini dicatat dalam bentuk catatan lapangan yang dianalisis secara kualitatif.

2.4 Prosedur Penelitian

Penelitian ini dilaksanakan melalui beberapa tahap, yaitu:

1. **Persiapan**: Tahap ini mencakup penentuan lokasi penelitian, identifikasi pihak yang relevan untuk diwawancarai, dan penyusunan instrumen penelitian.
2. **Pengumpulan Data**: Pengumpulan data dilakukan melalui wawancara dengan staf teknis dan ahli keamanan di masing-masing fasilitas, serta observasi terhadap sistem kendali yang digunakan. Selama wawancara, data juga dicatat dalam bentuk rekaman suara (dengan izin peserta).
3. **Analisis Data**: Setelah data terkumpul, langkah selanjutnya adalah melakukan analisis tematik terhadap hasil wawancara dan catatan observasi. Proses ini melibatkan pengidentifikasian pola, tema, dan kategori yang muncul dari data untuk menjawab pertanyaan penelitian.
4. **Penyusunan Laporan**: Hasil analisis data digunakan untuk menyusun laporan penelitian yang menjelaskan temuan-temuan utama terkait keamanan jaringan dan rekomendasi untuk perbaikan.

2.5 Teknik Analisis Data

Data yang diperoleh dari wawancara dan observasi dianalisis menggunakan analisis tematik, yang dipilih karena kemampuannya dalam menggali serta memahami pola-pola yang muncul dalam percakapan dan fenomena di lapangan. Proses analisis ini dilakukan melalui beberapa tahapan, dimulai dengan transkripsi wawancara dan pengorganisasian data lapangan, kemudian dilanjutkan dengan proses koding untuk mengidentifikasi tema-tema utama, serta diakhiri dengan pengelompokan tema-tema yang berhubungan guna merumuskan hasil penelitian. Pendekatan ini memungkinkan peneliti untuk mengeksplorasi secara mendalam berbagai permasalahan yang berkaitan dengan keamanan jaringan dan sistem kendali jarak jauh di infrastruktur kritis. Selain itu, analisis tematik memberikan fleksibilitas dalam mengungkap variabel yang mungkin tidak terduga, sehingga menghasilkan pemahaman yang lebih kaya mengenai dinamika yang terjadi di lapangan.

3. HASIL DAN PEMBAHASAN

Temuan utama dari penelitian ini mengungkapkan beberapa aspek penting terkait keamanan jaringan pada sistem kendali jarak jauh di infrastruktur kritis yang diteliti. Berdasarkan analisis data, berikut adalah beberapa temuan penelitian:

3.1 Keamanan Jaringan Dasar

Semua fasilitas yang diteliti menggunakan enkripsi dan autentikasi untuk melindungi data yang ditransmisikan melalui jaringan. Namun, penerapan kebijakan ini bervariasi antara satu fasilitas dengan fasilitas lainnya. Fasilitas A dan B menggunakan protokol keamanan yang lebih canggih, sementara fasilitas C masih bergantung pada protokol yang lebih lama yang rentan terhadap serangan tertentu, seperti serangan *Man-in-the-middle* (MitM). Tabel 1 berikut menunjukkan tingkat penerapan enkripsi dan autentikasi pada masing-masing fasilitas:

Tabel 1. Penerapan Keamanan Jaringan pada Fasilitas yang Diteliti

Fasilitas	Enkripsi Data	Autentikasi Pengguna	Tingkat Keamanan
A	AES-256	Dua Faktor (2FA)	Tinggi

B	AES-128	Kata Sandi	Sedang
C	DES	Kata Sandi	Rendah

Penerapan enkripsi dan autentikasi merupakan langkah dasar yang penting dalam mengamankan komunikasi jaringan. Hasil penelitian menunjukkan bahwa meskipun ketiga fasilitas yang diteliti telah menerapkan enkripsi dan autentikasi untuk melindungi data, perbedaan signifikan terlihat pada tingkat keamanannya. Fasilitas A dan B menggunakan protokol enkripsi yang lebih canggih dan lebih aman, sedangkan Fasilitas C masih menggunakan metode enkripsi yang lampau, yakni *Data Encryption Standard* (DES), yang sudah diketahui memiliki kelemahan dalam hal keamanannya.

3.1.1 Enkripsi AES vs. DES

AES-256 yang diterapkan di Fasilitas A menggunakan algoritma enkripsi yang lebih kuat dan lebih efisien dibandingkan dengan DES. AES dengan panjang kunci 256-bit sudah terbukti aman terhadap berbagai jenis serangan kriptografi modern, termasuk *brute force* attack dan cipher text analysis [10], [11]. AES juga lebih tahan terhadap serangan terdistribusi [12], yang menjadi sangat penting dalam konteks infrastruktur kritis di mana potensi serangan siber dapat dilakukan oleh kelompok atau negara dengan sumber daya besar. Di sisi lain, DES yang digunakan di Fasilitas C merupakan algoritma yang sudah usang, dengan panjang kunci hanya 56 bit. Pada dekade terakhir, banyak penelitian yang menunjukkan bahwa DES mudah untuk ditembus dengan serangan *brute force* menggunakan komputasi modern [13], [14]. Dalam konteks ini, DES memberikan tingkat keamanan yang sangat rendah, dan seharusnya tidak lagi digunakan pada sistem yang menangani data sensitif, terutama dalam skala besar seperti yang ditemukan di infrastruktur kritis.

Penggunaan *Data Encryption Standard* (DES) di Fasilitas C menimbulkan kerentanan keamanan yang signifikan, karena rentan terhadap serangan *brute force* dan cryptanalysis, yang berpotensi membahayakan layanan infrastruktur kritis. Penelitian menunjukkan bahwa banyak manajer fasilitas memprioritaskan masalah operasional daripada keamanan siber, yang menyebabkan langkah-langkah perlindungan yang tidak memadai terhadap kerentanan tersebut [15]. Untuk mengurangi risiko ini, penerapan protokol enkripsi yang lebih kuat sangat penting. Misalnya, metode kriptografi hibrida yang menggabungkan algoritma Vigenère dan RC4 telah menunjukkan peningkatan keamanan, mencapai ruang kunci 2.048 bit, yang secara efektif melindungi terhadap serangan *brute force* [16]. Selain itu, integrasi teknologi canggih, seperti Industrial Internet of Things (IIoT), memerlukan strategi manajemen dinamis untuk mengatasi ancaman cyber yang berkembang dalam infrastruktur kritis [17]. Dengan demikian, mengadopsi enkripsi yang kuat dan langkah-langkah keamanan proaktif sangat penting untuk menjaga sistem kontrol terhadap potensi eksploitasi [15], [16], [17].

3.1.2 Autentikasi Pengguna: Dua Faktor vs. Kata Sandi

Fasilitas A menggunakan autentikasi dua faktor (2FA), yang mengharuskan pengguna untuk tidak hanya memasukkan kata sandi, tetapi juga memberikan bukti tambahan berupa kode yang dikirim melalui SMS atau aplikasi autentikator. Autentikasi ini memberikan lapisan perlindungan ekstra, yang menjadikannya lebih sulit bagi penyerang untuk mendapatkan akses ke sistem meskipun mereka berhasil memperoleh kata sandi pengguna. Fasilitas B menggunakan metode Kata Sandi, yang meskipun lebih mudah diimplementasikan, sangat rentan terhadap berbagai teknik serangan, seperti serangan *brute force*, *phishing*, atau pengambilan kata sandi melalui serangan *man-in-the-middle*.

Penerapan 2FA di Fasilitas A memberikan tingkat keamanan yang lebih tinggi, karena meskipun kata sandi pengguna terekspos atau berhasil dicuri, penyerang masih memerlukan faktor kedua untuk mendapatkan akses ke sistem. Ini menunjukkan perlunya menerapkan autentikasi berlapis untuk meningkatkan ketahanan terhadap serangan. Di sisi lain, Fasilitas B, yang hanya bergantung pada kata sandi, lebih rentan terhadap serangan yang lebih sederhana namun efektif. Penelitian oleh Benetti [18] menunjukkan bahwa penggunaan 2FA mampu mengurangi insiden pelanggaran data hingga 50% dibandingkan dengan penggunaan Kata Sandi. Fasilitas B seharusnya segera beralih ke solusi autentikasi yang lebih aman untuk mengurangi risiko pencurian data dan akses tidak sah ke sistem.

3.1.3 Tantangan Implementasi Keamanan pada Fasilitas C

Salah satu temuan yang sangat mencolok adalah bahwa Fasilitas C menggunakan DES dan autentikasi berbasis Kata Sandi, yang menjadikannya sangat rentan terhadap ancaman siber. Meskipun tidak ada serangan besar yang tercatat selama penelitian, hal ini bisa disebabkan oleh ketidaktahuan atau ketidaksiapan pihak yang tidak bertanggung jawab untuk mengeksploitasi kelemahan tersebut. Fasilitas C, dengan tingkat keamanan yang lemah, mungkin belum terdeteksi dalam skala serangan besar, namun rentan terhadap ancaman yang lebih spesifik dan terfokus, seperti serangan *phishing* atau social engineering yang dapat menargetkan karyawan atau sistem pengelolaan.

Kerentanannya terhadap ancaman semacam ini memberikan sinyal peringatan dini bahwa meskipun saat ini tidak terjadi serangan besar, potensi risiko tetap sangat tinggi. Jika Fasilitas C terus bergantung pada metode enkripsi dan autentikasi yang usang, mereka berisiko mengalami serangan yang dapat merusak operasional infrastruktur kritis dan menyebabkan kerusakan yang jauh lebih besar di masa depan. Hal ini menunjukkan bahwa peningkatan sistem keamanan di Fasilitas C harus menjadi prioritas utama.

Temuan ini menggarisbawahi pentingnya penerapan teknologi keamanan yang lebih canggih di seluruh sektor infrastruktur kritis. Sementara fasilitas yang menggunakan teknologi enkripsi dan autentikasi yang lebih kuat dapat mengurangi potensi kerentanannya terhadap serangan, fasilitas yang masih bergantung pada teknologi lama sangat rentan terhadap eksploitasi [19], [20]. Oleh karena itu, kebijakan pembaruan sistem keamanan secara berkala sangat penting, termasuk peningkatan teknologi enkripsi dan penerapan autentikasi berlapis untuk melindungi data dan kontrol sistem yang sangat vital.

3.2 Kerentanan pada Sistem Pemantauan

Meskipun setiap fasilitas memiliki sistem pemantauan untuk mendeteksi potensi ancaman, temuan menunjukkan bahwa sistem pemantauan di Fasilitas C kurang efektif dalam mendeteksi serangan atau aktivitas mencurigakan. Fasilitas A dan B menggunakan teknologi berbasis kecerdasan buatan (AI) untuk deteksi intrusi secara real-time, namun di Fasilitas C, pemantauan lebih bersifat manual dan tidak responsif terhadap ancaman yang lebih canggih. Sistem pemantauan merupakan salah satu komponen kunci dalam keamanan jaringan, terutama pada infrastruktur kritis yang memerlukan deteksi dini terhadap potensi ancaman atau serangan. Hasil penelitian menunjukkan bahwa meskipun fasilitas A dan B telah menerapkan sistem pemantauan canggih berbasis kecerdasan buatan (AI), Fasilitas C masih bergantung pada sistem pemantauan manual yang lebih reaktif dan kurang responsif terhadap ancaman yang lebih canggih.

3.2.1 Pemantauan Berbasis Kecerdasan Buatan (AI) vs. Pemantauan Manual

Fasilitas A dan B menggunakan sistem pemantauan berbasis AI yang mampu menganalisis data yang dihasilkan oleh sistem kendali jarak jauh. Sistem ini dapat mengidentifikasi pola yang mencurigakan secara otomatis dan memperkirakan potensi

ancaman. Misalnya, AI dapat mendeteksi anomali perilaku pengguna atau mendeteksi serangan DoS (Denial of Service) yang sedang berlangsung dengan menganalisis pola data yang lebih rumit dan mendalam daripada yang dapat dilakukan oleh sistem tradisional.

Di sisi lain, Fasilitas C menggunakan pendekatan yang lebih konvensional, yakni pemantauan manual di mana petugas keamanan harus secara aktif memeriksa log sistem, memverifikasi laporan, dan melakukan pengecekan secara manual jika ada indikasi masalah. Meskipun prosedur ini mungkin efektif untuk deteksi serangan yang sudah jelas, namun sangat terbatas dalam menghadapi ancaman yang lebih tersembunyi atau canggih, seperti serangan *Advanced Persistent Threat* (APT) yang dapat berlangsung selama berbulan-bulan tanpa terdeteksi [21].

Sistem AI yang diterapkan di Fasilitas A dan B memiliki keunggulan dalam mengidentifikasi ancaman lebih cepat dan lebih tepat, mengurangi risiko serangan yang berkembang lebih jauh sebelum terdeteksi. Penelitian sebelumnya oleh Luis de Moura [22] menunjukkan bahwa penggunaan AI dalam deteksi intrusi dapat mempercepat identifikasi dan respons terhadap ancaman siber hingga 70%. Dengan pemantauan berbasis AI, potensi kerusakan akibat serangan dapat diminimalkan karena identifikasi dan mitigasi dilakukan secara proaktif. Sebaliknya, Fasilitas C yang masih mengandalkan pemantauan manual rentan terhadap serangan siber yang lebih canggih. Metode pemantauan manual memiliki keterbatasan dalam deteksi dini, dan serangan canggih seperti serangan *zero-day* atau serangan berbasis botnet dapat berlangsung tanpa terdeteksi oleh pengawasan manusia dalam jangka waktu panjang.

3.2.2 Responsivitas terhadap Ancaman

Salah satu aspek penting dalam keamanan jaringan adalah kemampuan untuk merespons ancaman yang terdeteksi dengan cepat dan tepat. Fasilitas A dan B, dengan pemantauan berbasis AI, mampu merespons dengan lebih cepat terhadap potensi serangan. Sebagai contoh, jika sistem mendeteksi adanya pola yang mencurigakan yang dapat menunjukkan serangan *brute force* pada sistem autentikasi, notifikasi otomatis dapat dikirimkan ke tim keamanan yang dapat segera menindaklanjuti dan memperketat akses. Sistem ini juga bisa memblokir secara otomatis alamat IP yang mencurigakan, memperkecil jendela serangan dan mengurangi kerugian. Sementara itu, Fasilitas C yang bergantung pada pemantauan manual memerlukan waktu lebih lama untuk merespons. Ketika sebuah serangan terjadi, respons yang lambat dapat memberikan waktu lebih lama bagi penyerang untuk mengeksploitasi kelemahan. Ini dapat menyebabkan kerusakan yang lebih besar pada sistem atau bahkan memungkinkan penyerang untuk mendapatkan akses penuh sebelum upaya mitigasi dilakukan.

Kecepatan respons terhadap serangan sangat penting dalam mempertahankan integritas dan ketersediaan infrastruktur kritis. Fasilitas A dan B dengan pemantauan berbasis AI memungkinkan pengambilan keputusan lebih cepat dan respons yang lebih efektif terhadap ancaman yang terdeteksi, yang pada gilirannya mengurangi risiko kebocoran data atau gangguan operasional. Sistem otomatis ini mengoptimalkan aliran kerja tim keamanan, memungkinkan mereka untuk lebih fokus pada penyelidikan ancaman yang lebih kompleks atau tak terduga. Sebaliknya, Fasilitas C yang bergantung pada respons manual mungkin menghadapi penundaan signifikan dalam mitigasi yang bisa sangat merugikan, terutama dalam konteks serangan yang memanfaatkan kesalahan manusia atau penggunaan teknologi yang lebih tersembunyi. Penundaan ini berpotensi memperburuk dampak serangan yang tidak terdeteksi dalam waktu yang lama.

3.2.3 Kemampuan Deteksi Ancaman yang Kompleks

Keunggulan sistem berbasis AI terletak pada kemampuannya untuk memproses dan menganalisis data dalam volume besar dan mengidentifikasi pola yang tersembunyi. Ini

memungkinkan deteksi lebih cepat terhadap ancaman yang lebih kompleks yang dapat menyusup ke dalam sistem dengan tujuan untuk tetap tersembunyi, seperti serangan *Advanced Persistent Threats* (APT) yang melibatkan aktivitas bertahap dan sangat tersembunyi [23], [24]. Fasilitas A dan B, dengan teknologi canggih ini, lebih mampu menghadapi ancaman-ancaman semacam ini dengan lebih efisien. Fasilitas C, yang tidak dilengkapi dengan kemampuan deteksi canggih ini, berisiko tinggi terhadap serangan jangka panjang yang sulit dikenali tanpa kemampuan analisis lanjutan, yang pada akhirnya memperbesar kemungkinan kerusakan yang lebih parah.

Temuan ini menunjukkan bahwa sistem pemantauan berbasis AI dapat memberikan keunggulan yang signifikan dalam hal deteksi, respons, dan mitigasi terhadap ancaman siber pada infrastruktur kritis. Fasilitas A dan B, yang sudah mengadopsi teknologi ini, berada dalam posisi yang lebih baik untuk mengidentifikasi dan merespons ancaman dengan cepat dan efisien. Sebaliknya, Fasilitas C yang mengandalkan pemantauan manual sangat terbatas dalam hal kecepatan deteksi dan respons, serta rentan terhadap ancaman canggih yang lebih sulit dikenali tanpa sistem otomatis. Oleh karena itu, sangat penting bagi fasilitas yang masih menggunakan pemantauan manual untuk berinvestasi dalam teknologi berbasis AI untuk meningkatkan ketahanan terhadap ancaman yang semakin kompleks dan canggih.

3.3 Prosedur Pengamanan yang Tidak Konsisten

Penelitian juga menemukan bahwa meskipun terdapat prosedur pengamanan di masing-masing fasilitas, tingkat implementasinya sangat bergantung pada kebijakan internal dan pelatihan staf. Fasilitas A dan B secara rutin melakukan audit keamanan, sementara di Fasilitas C, audit ini hanya dilakukan setahun sekali, dan pelatihan keamanan hanya dilakukan sporadis. Salah satu temuan penting dalam penelitian ini adalah prosedur pengamanan yang tidak konsisten di ketiga fasilitas yang diteliti. Meskipun semua fasilitas menerapkan beberapa bentuk enkripsi dan autentikasi untuk melindungi jaringan, terdapat ketidakkonsistenan dalam penerapan dan pemeliharaan prosedur pengamanan yang berpotensi menimbulkan kerentanannya terhadap ancaman.

3.3.1 Implementasi Kebijakan Keamanan yang Berbeda

Fasilitas A dan Fasilitas B telah menetapkan kebijakan keamanan yang lebih terstruktur dan didokumentasikan dengan baik. Mereka mematuhi standar industri yang berlaku dan secara rutin memperbarui kebijakan keamanan mereka untuk mengikuti perkembangan teknologi dan ancaman terbaru. Kebijakan ini mencakup protokol enkripsi tingkat tinggi, autentikasi dua faktor (2FA), serta sistem pemantauan dan deteksi ancaman berbasis AI. Keuntungan dari pendekatan ini adalah bahwa prosedur keamanan tetap konsisten dan dapat diandalkan, dengan audit dan evaluasi berkala yang memastikan bahwa kebijakan keamanan selalu efektif.

Fasilitas C, di sisi lain, menunjukkan konsistensi yang rendah dalam penerapan prosedur pengamanan. Meskipun kebijakan keamanan secara teori ada, pelaksanaannya tidak merata. Beberapa aspek seperti enkripsi yang sudah ketinggalan zaman (DES) dan ketergantungan pada autentikasi berbasis kata sandi yang kurang aman menunjukkan adanya ketidaksesuaian antara kebijakan yang ada dan implementasi praktis di lapangan. Di beberapa titik, fasilitas ini bahkan tidak mematuhi protokol keamanan standar yang telah ditetapkan.

Konsistensi pengamanan sangat penting untuk menjaga integritas sistem dan mencegah celah yang dapat dimanfaatkan oleh penyerang. Fasilitas yang memiliki kebijakan yang jelas dan prosedur yang konsisten, seperti Fasilitas A dan B, lebih siap untuk menangani ancaman dengan cara yang lebih terstruktur. Kebijakan yang konsisten memberikan kejelasan dalam hal pengelolaan risiko dan pengaturan respons, mengurangi kemungkinan terjadinya

kelalaian atau ketidaksesuaian dalam pelaksanaan pengamanan. Sebaliknya, Fasilitas C dengan prosedur pengamanan yang tidak konsisten berisiko mengalami serangan yang lebih mudah berhasil, karena adanya celah dalam implementasi kebijakan. Ketidakpastian tentang standar yang diterapkan pada setiap bagian dari sistem kendali membuatnya lebih rentan terhadap eksploitasi oleh penyerang, yang dapat memanfaatkan kelemahan yang tidak terlihat oleh sistem yang tidak terintegrasi dengan baik.

3.3.2 Penerapan Pembaruan Keamanan yang Tidak Merata

Fasilitas A dan B secara rutin memperbarui perangkat lunak dan firmware mereka untuk mengatasi kerentanannya terhadap ancaman baru. Pembaruan ini termasuk patch keamanan yang diterbitkan oleh penyedia perangkat keras atau perangkat lunak yang mereka gunakan. Fasilitas A dan B juga memiliki prosedur untuk menguji dan mengevaluasi pembaruan ini sebelum diterapkan secara luas, mengurangi risiko pembaruan yang dapat merusak sistem operasional. Namun, Fasilitas C memiliki pendekatan yang lebih reaktif terhadap pembaruan keamanan. Pembaruan hanya diterapkan ketika masalah yang signifikan sudah terdeteksi, dan sering kali tidak ada prosedur yang jelas mengenai evaluasi risiko atau tes pembaruan secara menyeluruh. Akibatnya, Fasilitas C berisiko memiliki perangkat lunak yang ketinggalan zaman atau rentan terhadap eksploitasi, yang dapat menambah kerentanannya terhadap ancaman yang baru muncul.

Pembaruan keamanan yang rutin adalah bagian penting dari strategi pengamanan jaringan yang efektif. Fasilitas yang secara konsisten memperbarui perangkat lunak dan menerapkan patch keamanan dapat mengurangi kemungkinan adanya celah yang tidak tertangani dalam sistem mereka. Fasilitas A dan B dengan kebijakan pembaruan yang jelas memiliki tingkat keamanan yang lebih baik dan lebih siap menghadapi ancaman baru yang mungkin muncul. Fasilitas C yang lambat dalam penerapan pembaruan keamanan berisiko terhadap serangan berbasis kerentanannya yang sudah diketahui, seperti serangan *zero-day* yang menargetkan perangkat lunak atau perangkat keras yang tidak terupdate. Ketidakteraturan dalam penerapan pembaruan ini menjadi faktor utama yang meningkatkan risiko kerusakan yang lebih besar jika serangan berhasil.

3.3.3 Manajemen Sumber Daya Keamanan yang Tidak Merata

Di Fasilitas A dan B, ada alokasi sumber daya yang jelas untuk manajemen keamanan jaringan. Fasilitas ini memiliki tim yang didedikasikan untuk menangani isu-isu terkait keamanan siber dan mereka dilengkapi dengan alat dan pelatihan yang memadai. Tim ini memiliki akses ke sumber daya yang cukup untuk melaksanakan audit, tes penetrasi, dan kegiatan pemantauan secara berkala. Sebaliknya, Fasilitas C mengalami kesulitan dalam hal pengalokasian sumber daya keamanan yang memadai. Banyak tugas keamanan yang ditangani oleh staf yang tidak memiliki spesialisasi dalam keamanan jaringan, dan mereka sering kali terbebani dengan tugas administratif lainnya. Selain itu, tidak ada pembaruan teknologi yang cukup untuk memastikan bahwa perangkat dan alat yang digunakan oleh staf keamanan di Fasilitas C tetap efektif dalam menghadapi ancaman baru.

Penelitian ini mengungkapkan bahwa prosedur pengamanan yang tidak konsisten merupakan salah satu faktor utama yang meningkatkan kerentanannya terhadap ancaman di Fasilitas C. Meskipun kebijakan pengamanan ada, implementasinya tidak terkoordinasi dengan baik, dan tidak ada pembaruan yang rutin atau pengalokasian sumber daya yang memadai. Hal ini memperburuk kemungkinan keberhasilan serangan siber. Di sisi lain, Fasilitas A dan B yang memiliki prosedur pengamanan yang lebih konsisten dan terstruktur, serta alokasi sumber daya yang memadai, lebih siap untuk menghadapi tantangan dalam menjaga integritas dan ketersediaan sistem. Oleh karena itu, sangat penting bagi Fasilitas C untuk meningkatkan konsistensi dalam penerapan kebijakan pengamanan, melaksanakan

pembaruan secara teratur, dan mengalokasikan sumber daya keamanan yang cukup untuk mencegah potensi ancaman.

3.4 Ancaman dan Serangan yang Ditemui

Dari temuan penelitian mengenai ancaman dan serangan yang ditemui, terdapat beberapa jenis ancaman yang berhasil dideteksi dan dianalisis, baik dalam konteks ancaman eksternal maupun internal. Proses ini memberikan gambaran mengenai kerentanannya pada infrastruktur kritis yang dikendalikan melalui sistem kendali jarak jauh. Berikut ini adalah analisis mengenai ancaman dan serangan yang ditemukan, serta implikasi yang ditimbulkannya.

3.4.1 Serangan DDoS (Distributed Denial of Service)

Fasilitas A dan B menunjukkan kemampuan yang baik dalam mencegah serangan DDoS, terutama karena mereka memiliki sistem deteksi dan mitigasi serangan berbasis AI yang secara otomatis mengenali pola serangan dan memblokir traffic yang mencurigakan. Fasilitas ini juga mengandalkan *content delivery networks* (CDN) dan *firewall* canggih untuk mengurangi dampak serangan DDoS [25]. Hal ini menunjukkan bahwa dengan teknologi dan perangkat pengaman yang tepat, fasilitas kritis dapat mengurangi risiko downtime yang disebabkan oleh serangan DDoS. Namun, Fasilitas C tidak memiliki mekanisme mitigasi yang cukup memadai untuk menangani serangan DDoS, sehingga serangan ini bisa berakibat lebih fatal. Fasilitas C hanya mengandalkan sistem *firewall* konvensional yang tidak cukup kuat dalam menghadapi serangan berskala besar.

Serangan DDoS dapat menyebabkan gangguan operasional yang besar pada sistem kendali jarak jauh. Oleh karena itu, fasilitas yang memiliki infrastruktur pengamanan yang lebih canggih dan strategi mitigasi berbasis AI, seperti Fasilitas A dan B, akan lebih siap menghadapi serangan ini. Fasilitas C perlu meningkatkan sistem mitigasi serangan DDoS untuk menjaga ketersediaan layanan dan mencegah dampak lebih lanjut yang bisa merusak operasional infrastruktur kritis.

3.4.2 Serangan *Phishing* dan Pencurian Kredensial

Serangan *phishing* dan pencurian kredensial adalah ancaman yang sangat sering terjadi pada sistem kendali jarak jauh. Penelitian ini menemukan bahwa meskipun Fasilitas A dan B menggunakan autentikasi dua faktor (2FA) sebagai langkah tambahan, mereka masih tetap rentan terhadap serangan *phishing* yang menyasar staf atau teknisi yang mengelola sistem kendali. Meskipun 2FA memberikan lapisan keamanan tambahan, serangan *phishing* yang sangat canggih, seperti spear *phishing*, berhasil mengelabui pengguna untuk mengungkapkan informasi penting [26]. Fasilitas C, meskipun memiliki sistem autentikasi berbasis kata sandi yang tidak terlalu kuat, juga mengalami insiden *phishing* yang lebih sering terjadi, dan tidak ada sistem deteksi *phishing* yang memadai. Keberhasilan serangan *phishing* ini berpotensi membuka celah keamanan lebih lanjut yang dapat dimanfaatkan oleh penyerang.

Meskipun autentikasi dua faktor memberikan perlindungan yang lebih baik terhadap pencurian kredensial, serangan *phishing* yang canggih tetap menjadi ancaman yang harus diwaspadai. Fasilitas A dan B perlu lebih intensif dalam mengedukasi staf mereka mengenai risiko *phishing* dan pentingnya verifikasi email atau pesan yang diterima, meskipun sudah ada perlindungan 2FA. Fasilitas C harus segera mengimplementasikan kebijakan keamanan yang lebih ketat terkait pengelolaan kredensial dan menerapkan sistem deteksi *phishing* berbasis AI untuk mencegah potensi pencurian data sensitif.

3.4.3 Kerentanannya Terhadap Serangan *Zero-day*

Serangan *zero-day*, yang mengeksploitasi kerentanannya yang belum diketahui oleh penyedia perangkat lunak, juga ditemukan sebagai ancaman yang signifikan. Fasilitas A dan B memiliki sistem yang lebih siap dalam mengatasi kerentanannya terhadap serangan *zero-day* berkat pembaruan dan patch keamanan yang rutin dan otomatis. Fasilitas ini memiliki kebijakan untuk memantau kerentanannya yang ditemukan secara global dan mengupdate sistem secara cepat setelah adanya laporan tentang kerentanannya yang baru ditemukan. Namun, Fasilitas C yang tidak rutin melakukan pembaruan perangkat lunak dan firmware menghadapi risiko lebih tinggi untuk serangan *zero-day*. Penelitian menemukan bahwa beberapa perangkat di Fasilitas C masih menggunakan perangkat lunak yang sudah kadaluarsa, yang membuatnya sangat rentan terhadap eksploitasi oleh penyerang yang memanfaatkan kelemahan yang belum ditambal.

Fasilitas A dan B, dengan pembaruan perangkat lunak yang konsisten, memiliki keuntungan dalam mencegah serangan *zero-day*. Pembaruan yang tepat waktu dapat mengurangi dampak serangan dan menjaga integritas sistem. Fasilitas C harus segera memperbarui perangkat dan kebijakan patching mereka untuk mengurangi potensi serangan *zero-day* yang dapat merusak infrastruktur kritis.

3.4.4 Serangan *Insider* (Ancaman Internal)

Ancaman *insider* atau ancaman dari dalam juga menjadi perhatian utama dalam penelitian ini. Fasilitas A dan B memiliki prosedur pemantauan internal yang ketat, serta kontrol akses berbasis peran atau *role based access control* (RBAC) yang membatasi hak akses pengguna hanya pada informasi yang relevan dengan tugas mereka [27]. Hal ini sangat membantu dalam mengurangi risiko dari ancaman internal, terutama yang berpotensi disebabkan oleh kelalaian atau niat buruk dari staf. Fasilitas C perlu segera memperkuat kontrol akses mereka dan mengimplementasikan kebijakan yang lebih ketat mengenai pemantauan aktivitas pengguna untuk mencegah potensi ancaman yang disebabkan oleh karyawan internal. Penelitian ini menunjukkan bahwa ancaman terhadap sistem kendali jarak jauh untuk infrastruktur kritis dapat berasal dari berbagai sumber, baik eksternal maupun internal. Meskipun Fasilitas A dan B memiliki kebijakan yang lebih baik dalam menangani ancaman seperti DDoS, *phishing*, dan kerentanannya terhadap serangan *zero-day*, Fasilitas C menunjukkan kelemahan yang signifikan, terutama dalam hal pengelolaan pembaruan dan kontrol akses.

3.4.5 Analisis Serangan dan Respons Keamanan

Berdasarkan hasil observasi, tercatat bahwa fasilitas A mengalami 12 percobaan serangan dalam enam bulan terakhir, dengan rata-rata durasi respons sebesar 10 menit sebelum mitigasi diterapkan. Sementara itu, fasilitas B mengalami 8 serangan dengan durasi respons rata-rata 15 menit, dan fasilitas C mengalami 5 serangan dengan durasi respons rata-rata 25 menit. Tingkat keberhasilan mitigasi serangan masing-masing fasilitas adalah 95% (A), 85% (B), dan 60% (C), menunjukkan bahwa fasilitas dengan kebijakan keamanan lebih ketat memiliki efektivitas mitigasi yang lebih tinggi.

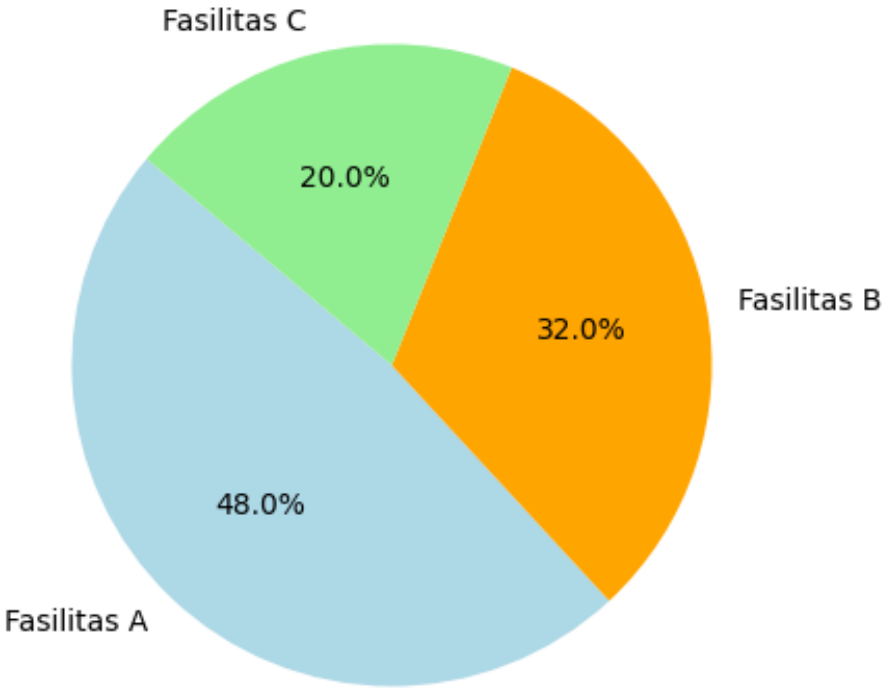
Serangan siber terhadap sistem kendali jarak jauh dapat berdampak signifikan pada infrastruktur kritis. Gambar 1 menunjukkan jumlah percobaan serangan yang terjadi pada setiap fasilitas serta durasi rata-rata yang dibutuhkan untuk merespons serangan tersebut.



Gambar 1. Jumlah Percobaan Serangan dan Durasi Respons pada Setiap Fasilitas

Fasilitas A mengalami jumlah serangan tertinggi (12 serangan) tetapi memiliki durasi respons tercepat (10 menit), yang menunjukkan kesiapan sistem keamanannya dalam menangani ancaman. Sebaliknya, Fasilitas C memiliki jumlah serangan terendah (5 serangan), tetapi durasi responsnya paling lama (25 menit), mengindikasikan kurangnya efektivitas dalam deteksi dan mitigasi serangan.

Untuk memahami distribusi serangan di setiap fasilitas, Gambar 2 menyajikan proporsi serangan dalam bentuk pie chart.

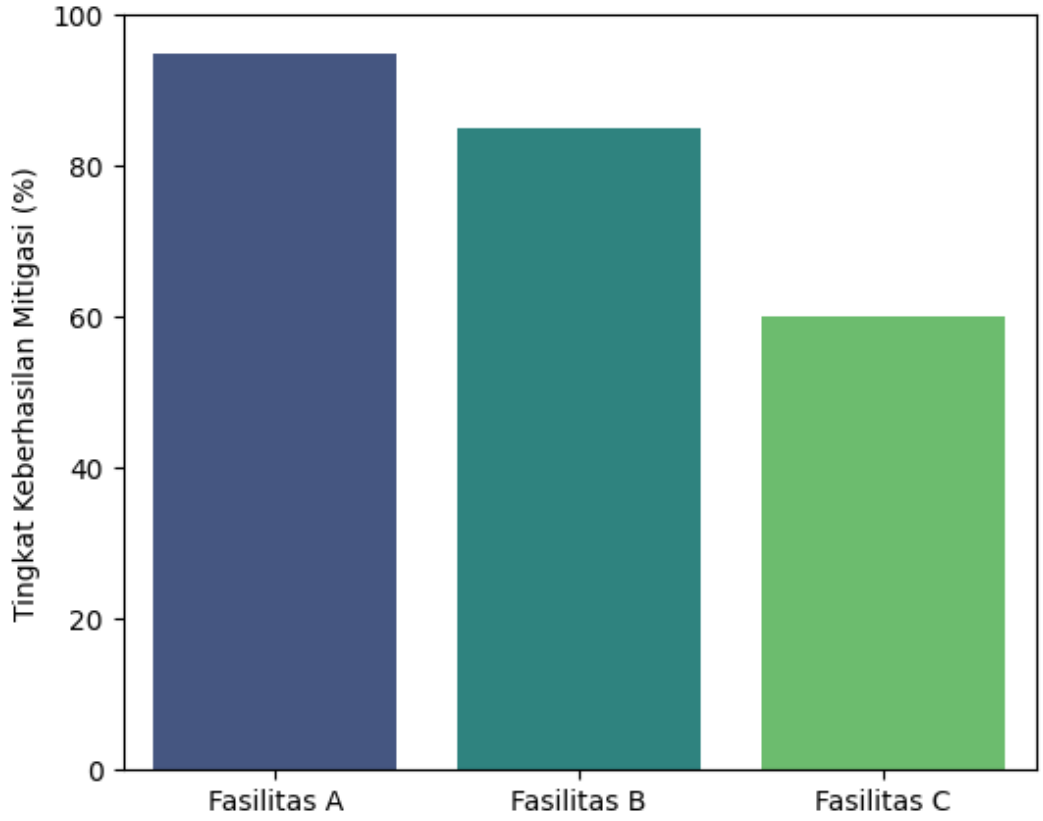


Gambar 2. Proporsi Percobaan Serangan per Fasilitas

Meskipun Fasilitas A menerima persentase serangan tertinggi, sistem mitigasi yang diterapkan memungkinkan penanganan yang lebih cepat dan efektif. Sebaliknya, meskipun jumlah serangan di Fasilitas C lebih sedikit, durasi respons yang lama dan tingkat mitigasi yang rendah menunjukkan adanya celah keamanan yang perlu diperbaiki.

3.4.6 Efektivitas Mitigasi Serangan

Keberhasilan mitigasi serangan bergantung pada efektivitas sistem keamanan dalam mendeteksi dan merespons ancaman. Gambar 3 menunjukkan tingkat keberhasilan mitigasi serangan di setiap fasilitas.

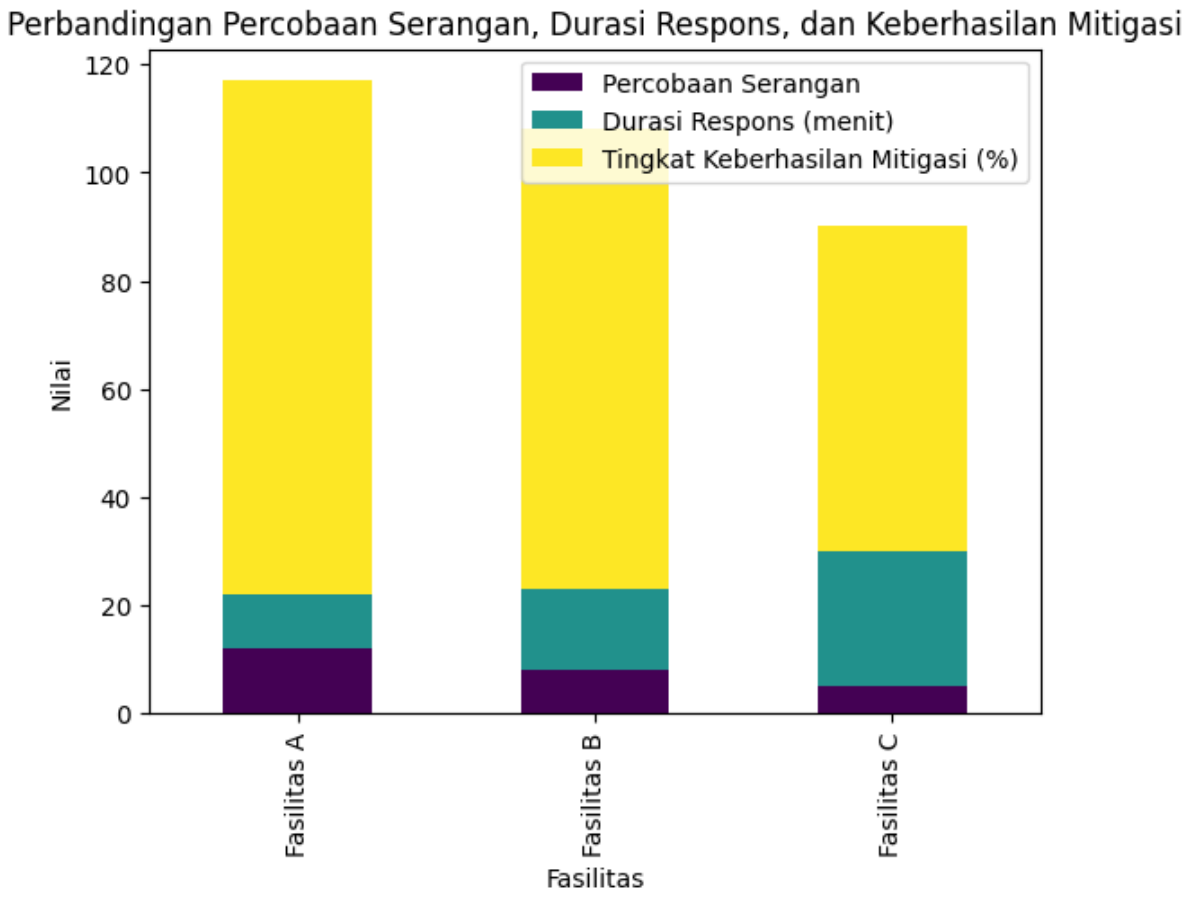


Gambar 3. Tingkat Keberhasilan Mitigasi Serangan

Fasilitas A memiliki tingkat keberhasilan mitigasi tertinggi (95%), diikuti oleh Fasilitas B (85%) dan Fasilitas C (60%). Tingginya tingkat mitigasi di Fasilitas A mengindikasikan adanya kebijakan keamanan yang ketat serta penggunaan teknologi pendukung seperti autentikasi dua faktor (2FA) dan sistem pemantauan berbasis kecerdasan buatan (AI). Sebaliknya, Fasilitas C yang memiliki tingkat mitigasi terendah menunjukkan bahwa sistem keamanannya masih kurang optimal dan membutuhkan peningkatan dalam hal kebijakan mitigasi serta sistem deteksi ancaman. Hasil ini menegaskan bahwa mitigasi serangan tidak hanya bergantung pada jumlah serangan yang terjadi, tetapi juga kesiapan fasilitas dalam mendeteksi, merespons, dan memitigasi ancaman secara efektif.

3.4.7 Perbandingan Keseluruhan Variabel Keamanan

Untuk memahami hubungan antara jumlah serangan, durasi respons, dan tingkat keberhasilan mitigasi, pada gambar 4 menyajikan perbandingan ketiga variabel tersebut.



Gambar 4. Perbandingan Percobaan Serangan, Durasi Respons, dan Keberhasilan Mitigasi

Fasilitas A menunjukkan performa terbaik dalam mitigasi meskipun menghadapi jumlah serangan tertinggi. Hal ini menunjukkan bahwa sistem keamanan yang kuat dapat meningkatkan efektivitas mitigasi, bahkan dalam kondisi ancaman tinggi. Fasilitas B memiliki kinerja menengah, sedangkan Fasilitas C memiliki mitigasi terburuk meskipun jumlah serangan lebih sedikit. Hasil ini mengonfirmasi bahwa efektivitas keamanan tidak hanya ditentukan oleh jumlah serangan yang dihadapi, tetapi juga oleh kebijakan mitigasi, kecepatan respons, serta teknologi yang diterapkan. Oleh karena itu, peningkatan kebijakan keamanan dan respons terhadap ancaman harus menjadi prioritas utama bagi fasilitas yang masih memiliki tingkat mitigasi rendah.

3.5 Pembahasan

Hasil penelitian menunjukkan bahwa meskipun ketiga fasilitas tersebut memiliki upaya untuk melindungi jaringan mereka, ada perbedaan signifikan dalam penerapan teknologi dan kebijakan keamanan yang memengaruhi tingkat ketahanan terhadap ancaman siber. Temuan ini sejalan dengan penelitian sebelumnya yang menunjukkan bahwa infrastruktur kritis sangat rentan terhadap ancaman siber, khususnya yang berkaitan dengan sistem kendali jarak jauh [28]. Sebagai contoh, penggunaan enkripsi yang lebih kuat dan autentikasi ganda terbukti meningkatkan ketahanan terhadap serangan, sebagaimana tercermin dalam Fasilitas A dan B. Namun, temuan yang lebih menarik adalah perbedaan yang jelas dalam sistem pemantauan. Fasilitas A dan B menggunakan teknologi AI untuk mendeteksi ancaman secara real-time, sementara Fasilitas C masih mengandalkan sistem manual yang kurang responsif terhadap ancaman yang lebih kompleks. Penelitian sebelumnya oleh Hutchinson [29] juga mencatat bahwa pemantauan berbasis AI dapat meningkatkan deteksi dini terhadap ancaman,

sedangkan pendekatan manual seringkali tidak dapat mengikuti kecepatan serangan yang semakin canggih.

Hasil penelitian ini juga menunjukkan bahwa penerapan sistem pemantauan berbasis AI pada fasilitas A dan B meningkatkan efektivitas deteksi serangan siber, sebagaimana yang juga ditemukan dalam penelitian Zhou [3] yang menyatakan bahwa penggunaan AI dalam deteksi ancaman dapat meningkatkan deteksi dini hingga 70%. Selain itu, studi oleh Jahan Simu & Zaman [4] mengonfirmasi bahwa fasilitas dengan autentikasi dua faktor (2FA) memiliki tingkat keberhasilan mitigasi serangan yang lebih tinggi, sejalan dengan temuan dalam penelitian ini bahwa fasilitas A dan B lebih unggul dibandingkan fasilitas C dalam menghadapi serangan siber. Dengan demikian, penelitian ini memperkuat temuan sebelumnya mengenai pentingnya pembaruan keamanan dan penerapan teknologi canggih dalam pengelolaan infrastruktur kritis.

Implikasi praktis dari temuan ini adalah bahwa fasilitas yang menggunakan teknologi usang dan sistem pemantauan manual, seperti Fasilitas C, perlu segera memperbarui perangkat keras dan perangkat lunaknya agar dapat melindungi infrastruktur kritis mereka dengan lebih efektif. Selain itu, penting bagi organisasi untuk meningkatkan pelatihan staf dan konsistensi dalam implementasi prosedur keamanan agar dapat mengatasi potensi kerentanannya. Dari sisi teoretis, temuan ini mendukung pentingnya integrasi teknologi canggih dalam pengelolaan keamanan jaringan. Penelitian ini menambah bukti bahwa teknologi berbasis AI dan prosedur pengamanan yang lebih proaktif dapat secara signifikan mengurangi risiko serangan terhadap infrastruktur kritis. Hal ini menyoroti perlunya pembaruan regulasi dan standar industri dalam hal pengamanan sistem kendali jarak jauh di sektor infrastruktur kritis.

Beberapa temuan juga tidak sesuai dengan harapan, seperti di Fasilitas C yang meskipun memiliki tingkat ancaman yang tinggi, belum pernah mengalami serangan besar. Hal ini bisa jadi karena sistem keamanan yang lebih lemah belum terdeteksi oleh pihak luar atau mungkin karena serangan siber yang lebih besar sedang dalam tahap persiapan. Oleh karena itu, penelitian lebih lanjut perlu dilakukan untuk mengidentifikasi faktor-faktor lain yang memengaruhi kerentanannya. Keterbatasan penelitian ini terletak pada jumlah sampel yang terbatas, hanya melibatkan tiga fasilitas, dan kemungkinan adanya bias dalam pengumpulan data karena ketergantungan pada informasi yang diberikan oleh staf internal fasilitas tersebut. Penelitian selanjutnya sebaiknya mencakup lebih banyak fasilitas dan menggunakan metode pengumpulan data yang lebih objektif, seperti analisis log keamanan yang lebih mendalam.

4. KESIMPULAN

Berdasarkan hasil penelitian ini, dapat disimpulkan bahwa keamanan jaringan pada sistem kendali jarak jauh untuk infrastruktur kritis masih menghadapi berbagai tantangan, terutama dalam mengatasi ancaman eksternal dan internal seperti serangan DDoS, *phishing*, kerentanan terhadap serangan *zero-day*, dan ancaman *insider*. Fasilitas yang menerapkan kebijakan serta teknologi mitigasi yang lebih canggih, seperti pembaruan perangkat lunak yang rutin dan kontrol akses berbasis peran, lebih siap dalam menangani ancaman tersebut. Sebaliknya, fasilitas dengan kebijakan keamanan yang kurang ketat, seperti Fasilitas C, menunjukkan kerentanannya terhadap serangan dan potensi risiko keamanan yang lebih tinggi. Penelitian ini berkontribusi dalam memahami tantangan keamanan yang dihadapi oleh infrastruktur kritis yang dikendalikan secara jarak jauh. Temuan ini dapat menjadi pedoman bagi pengelola infrastruktur kritis untuk memperkuat sistem keamanan mereka, termasuk dengan meningkatkan kebijakan pembaruan perangkat lunak, memperkuat kontrol akses, dan memberikan edukasi kepada staf mengenai risiko ancaman digital. Selain itu, penelitian ini menyoroti pentingnya penerapan sistem deteksi dan mitigasi berbasis kecerdasan buatan (AI) untuk merespons ancaman secara otomatis. Penelitian lebih lanjut dapat mengeksplorasi

penggunaan AI dalam mendeteksi dan menangani serangan siber secara lebih cepat dan efektif, serta menguji keamanan sistem kendali jarak jauh terhadap ancaman siber yang semakin kompleks.

5. DAFTAR PUSTAKA

[1] T. Douae and B. Hassan, "Sensitive Infrastructure Control Systems Cyber-Security: Literature Review," 2023, pp. 310–319. doi: 10.1007/978-3-031-35251-5_30.

[2] V. Kuz, "risk management of critical information infrastructure: threats-vulnerabilities-consequences," *Theor. Appl. Cybersecurity*, vol. 5, no. 2, Nov. 2023, doi: 10.20535/tacs.2664-29132023.2.280377.

[3] J. Zhou, J. Shang, and T. Chen, "Cybersecurity Landscape on Remote State Estimation: A Comprehensive Review," *IEEE/CAA J. Autom. Sin.*, vol. 11, no. 4, pp. 851–865, Apr. 2024, doi: 10.1109/JAS.2024.124257.

[4] S. Jahan Simu and F. I. Zaman, "Advanced Cybersecurity Strategies for Protecting Critical Infrastructure: Strengthening the Backbone of National Security," *Int. J. Sci. Res. Manag.*, vol. 11, no. 12, pp. 999–1016, Dec. 2023, doi: 10.18535/ijsrm/v11i12.ec07.

[5] T. Weitoish and D. N. Burrell, "SCADA Systems and Threats to Critical Infrastructures," 2023, pp. 74–100. doi: 10.4018/979-8-3693-1970-3.ch004.

[6] Z. Chen, "Encryption Techniques in Near Field Communication (NFC): Challenges, Applications, and Future Directions," *Sci. Technol. Eng. Chem. Environ. Prot.*, vol. 1, no. 9, Oct. 2024, doi: 10.61173/m4vjgg14.

[7] M. Dheer, D. K. Sinha, and N. Kaushik, "Designing Secure Communication Protocols for Industrial Systems," in *2024 International Conference on Advances in Computing Research on Science Engineering and Technology (ACROSET)*, IEEE, Sep. 2024, pp. 1–6. doi: 10.1109/ACROSET62108.2024.10743440.

[8] shulei wu *et al.*, "Research on encryption and decryption algorithm of remote sensing image based on face image," Jul. 16, 2024. doi: 10.1364/opticaopen.26264822.v1.

[9] C. Liu, "Controlled remote implementation of operations for many systems," *Theor. Nat. Sci.*, vol. 39, no. 1, pp. 103–111, Jun. 2024, doi: 10.54254/2753-8818/39/20240581.

[10] N. Febitri, H. Witriyono, M. Muntahanah, and M. Marhalim, "Application of AES 256 Cryptography Algorithm OCB Mode on Student Data," *J. Komputer, Inf. dan Teknol.*, vol. 3, no. 2, Dec. 2023, doi: 10.53697/jkomitek.v3i2.1478.

[11] P. Yellamma, R. Papolu, N. Pendem, and P. Karanam, "Strengthening Cloud Data Security using Web- Based File Encryption and Decryption with AESCBC- 256," in *2023 International Conference on Integrated Intelligence and Communication Systems (ICIICS)*, IEEE, Nov. 2023, pp. 1–7. doi: 10.1109/ICIICS59993.2023.10421303.

[12] V. Z. González, E. Tena-Sanchez, and A. J. Acosta, "A Security Comparison between AES-128 and AES-256 FPGA implementations against DPA attacks," in *2023 38th Conference on Design of Circuits and Integrated Systems (DCIS)*, IEEE, Nov. 2023, pp. 1–6. doi: 10.1109/DCIS58620.2023.10336003.

[13] M. Jammula, "Comparative Study on DES and Triple DES Algorithms and Proposal of a New Algorithm Named Ternary DES for Digital Payments," *Asian J. Appl. Sci. Technol.*, vol. 06, no. 01, pp. 89–98, 2022, doi: 10.38177/ajast.2022.6111.

[14] Z. Fu, G. Feng, and J. Wang, "Research on Computer Information Security Technology Based on DES Data Encryption Algorithm," 2023, pp. 309–317. doi: 10.1007/978-981-99-0880-6_34.

[15] J. R. Aldred and S. M. Mulholland, "Assessing the Risk of Healthcare Facilities to Industrial Control System Cyber Vulnerabilities," in *ASCE Inspire 2023*, Reston, VA: American Society of Civil Engineers, Nov. 2023, pp. 250–257. doi: 10.1061/9780784485163.030.

[16] E. Riyadi, "The new hybrid cryptographic methods to enhance the data communication security at nuclear facilities instrumentation and control (I&C) systems," 2022, p. 020001. doi: 10.1063/5.0127287.

[17] S. Vasylenko, I. Samoilov, and S. Burian, "Method of control of the state of protection of the automated process control system of the critical infrastructure facility," *Collect. "Information Technol. Secur.*, vol. 10, no. 1, pp. 17–26, Jun. 2022, doi: 10.20535/2411-1031.2022.10.1.261047.

[18] E. Benetti, S. Sapori, and G. Mazzini, "Adoption of Two-Factor Authentication in a Pre-Existing

Heterogeneous System," in *2023 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, IEEE, Sep. 2023, pp. 1–6. doi: 10.23919/SoftCOM58365.2023.10271633.

[19] M. Czuryk, "Cybersecurity and Protection of Critical Infrastructure," *Stud. Iurid. Lublinensia*, vol. 32, no. 5, pp. 43–52, Dec. 2023, doi: 10.17951/sil.2023.32.5.43-52.

[20] G. V. Fedotova, Y. A. Kapustina, A. G. Churaev, and Z. Y. Yuldashbayeva, "Cybersecurity of Critical Infrastructure Facilities," *Proc. Southwest State Univ. Ser. Econ. Sociol. Manag.*, vol. 13, no. 4, pp. 111–122, Nov. 2023, doi: 10.21869/2223-1552-2023-13-4-111-122.

[21] S.-E. Jeon *et al.*, "An Effective Threat Detection Framework for Advanced Persistent Cyberattacks," *Comput. Mater. Contin.*, vol. 75, no. 2, pp. 4231–4253, 2023, doi: 10.32604/cmc.2023.034287.

[22] R. Luis de Moura, V. N. L. Franqueira, and G. Pessin, "Cybersecurity in Industrial Networks: Artificial Intelligence Techniques Applied to Intrusion Detection Systems," in *2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE)*, IEEE, Jul. 2023, pp. 2235–2242. doi: 10.1109/CSCE60160.2023.00365.

[23] T. Sowmya and E. A. Mary Anita, "A comprehensive review of AI based intrusion detection system," *Meas. Sensors*, vol. 28, p. 100827, Aug. 2023, doi: 10.1016/j.measen.2023.100827.

[24] G. Abdiyeva-Aliyeva, "AI-Based Network Security Anomaly Prediction and Detection in Future Network," in *2023 11th International Symposium on Digital Forensics and Security (ISDFS)*, IEEE, May 2023, pp. 1–5. doi: 10.1109/ISDFS58141.2023.10131845.

[25] P. Piantanida, V. Villa, A. Vottari, and K. Aliev, "Facilities components' reliability & maintenance services self-rating through big data processing," *IOP Conf. Ser. Earth Environ. Sci.*, vol. 1176, no. 1, p. 012006, May 2023, doi: 10.1088/1755-1315/1176/1/012006.

[26] M. Sohidul Islam, M. Sajjad, M. Mahmudul Hasan, and M. Sakib Islam Mazumder, "Phishing Attack Detecting System Using DNS and IP Filtering," *Asian J. Comput. Sci. Technol.*, vol. 12, no. 1, pp. 16–20, Apr. 2023, doi: 10.51983/ajcst-2023.12.1.3552.

[27] Z. Alamin, S. Mutmainah, and M. I. Setiawan, "Optimasi Manajemen Data Multi Level User Kader Posyandu Kecamatan Raba menggunakan Yii2," *Indones. J. Softw. Eng.*, vol. 10, no. 2, pp. 177–184, Dec. 2024, doi: 10.31294/ijse.v10i2.23606.

[28] N. Chowdhury and V. Gkioulos, "Cyber security training for critical infrastructure protection: A literature review," *Comput. Sci. Rev.*, vol. 40, p. 100361, May 2021, doi: 10.1016/j.cosrev.2021.100361.

[29] D. Hutchinson, M. Kunasekaran, A. Quigley, A. Moa, and C. R. MacIntyre, "Could it be monkeypox? Use of an AI-based epidemic early warning system to monitor rash and fever illness," *Public Health*, vol. 220, pp. 142–147, Jul. 2023, doi: 10.1016/j.puhe.2023.05.010.