JURNAL RESPONSIVE
Teknik Informatika

Juni 2025 | Vol. 9 | No. 01
E-ISSN : 2614-7602
DOI: 10.36352/jr.v9i01.1178

ANALISIS TANTANGAN KEAMANAN JARINGAN IOT DAN STRATEGI MITIGASINYA

Maria Triani Mbejo*[1], Indra Sufian[2]
[1,2]Program Studi Teknik Informatika, Fakultas Sains dan Teknologi - Universitas Ibnu Sina, Batam
e-mail: ***[1]231055201001@uis.ac.id** [2]indra.sufian@uis.ac.id

Abstrak

Pertumbuhan *Internet of Things* (IoT) yang pesat memperluas permukaan serangan siber, sedangkan tantangan keamanan, jenis serangan, dan strategi mitigasi dalam literatur umumnya dibahas secara terpisah. Penelitian ini bertujuan memetakan ketiganya secara terintegrasi melalui kajian literatur kualitatif terhadap 19 sumber yang terbit pada 2019–2025, dengan analisis deskriptif. Kajian ini mengidentifikasi empat tantangan utama, yaitu integritas data, autentikasi dan enkripsi yang lemah, segmentasi jaringan yang kurang memadai, serta pembaruan perangkat yang diabaikan. Tantangan tersebut dieksploitasi melalui serangan *Distributed Denial of Service* (DDoS) dan *Man-in-the-Middle* (MitM). Laporan Cloudflare mencatat 20,5 juta serangan DDoS pada kuartal pertama 2025; angka ini mencakup seluruh target serangan dan tidak khusus IoT. Kebaruan penelitian ini terletak pada tiga hal: (1) matriks pemetaan tantangan–serangan–mitigasi, (2) penempatan enam strategi mitigasi pada lapisan arsitektur IoT, dan (3) usulan prioritas mitigasi tiga tingkat berdasarkan cakupan perlindungan, beban terhadap perangkat, dan ketersediaan mitigasi pengganti. Hasil pemetaan menunjukkan bahwa MitM hanya memiliki satu mitigasi langsung, yaitu enkripsi, sehingga langkah dasar (kredensial, pembaruan *firmware*, segmentasi) diusulkan didahulukan sebelum enkripsi dan deteksi lanjutan. Usulan ini bersifat konseptual dan perlu diuji secara empiris.

Kata kunci: IoT, keamanan jaringan, DDoS, MitM, strategi mitigasi

Abstract

The rapid growth of the Internet of Things (IoT) enlarges the cyberattack surface, yet security challenges, attack types, and mitigation strategies are generally discussed separately in the literature. This study maps them in an integrated way through a qualitative literature review of 19 sources published in 2019–2025, using descriptive analysis. Four main challenges are identified: data integrity, weak authentication and encryption, inadequate network segmentation, and neglected device updates. These challenges are exploited through Distributed Denial of Service (DDoS) and Man-in-the-Middle (MitM) attacks. Cloudflare recorded 20.5 million DDoS attacks in the first quarter of 2025; this figure covers all targets and is not specific to IoT. The novelty of this study lies in three contributions: (1) a challenge–attack–mitigation mapping matrix, (2) the placement of six mitigation strategies on the IoT architecture layers, and (3) a proposed three-tier mitigation priority based on protection coverage, device resource burden, and the availability of alternative mitigations. The mapping shows that MitM has only one direct mitigation, namely encryption, so basic measures (credentials, firmware updates, segmentation) are proposed to come before encryption and advanced detection. The proposal is conceptual and requires empirical testing.

Keywords*—IoT, network security, DDoS, MitM, mitigation strategy*

PENDAHULUAN

Perkembangan *Internet of Things* (IoT) yang pesat menjadikannya bagian yang lazim dalam kehidupan sehari-hari. IoT menawarkan beragam layanan yang mempercepat adopsinya dan berdampak besar pada kehidupan sosial maupun lingkungan bisnis (Saini & Saini, 2019). Statista memproyeksikan sekitar 75,44 miliar perangkat IoT terpasang pada 2025. Di balik pertumbuhan tersebut, keamanan data dan jaringan belum sepenuhnya terjamin, dan masalah ini bukan hanya tantangan IoT, melainkan tantangan teknologi digital pada umumnya.

Istilah *Internet of Things* pertama kali dikenal pada 1999 dan dicetuskan oleh Kevin Ashton, ilmuwan komputer yang saat itu bekerja di Procter & Gamble. Ia memperkenalkannya dalam presentasi tentang penggunaan RFID untuk melacak produk dalam rantai pasokan (Netmonk, 2019). Para peneliti mendefinisikan IoT dengan istilah yang berbeda-beda, tetapi umumnya merujuk pada serangkaian perangkat yang saling terhubung dan dapat berkomunikasi (Thilakarthne dkk., 2025). Secara sederhana, IoT adalah jaringan perangkat yang memanfaatkan internet, baik melalui media kabel maupun nirkabel, untuk saling berkomunikasi dengan pola komunikasi *machine-to-machine* (M2M) (Thilakarthne dkk., 2025).

IoT telah mengubah hubungan manusia dengan teknologi dari hubungan yang semula tidak intens menjadi hubungan yang hampir tidak terpisahkan dari keseharian. IoT memungkinkan perangkat elektronik di sekitar kita menjadi bagian dari satu jaringan terintegrasi dan telah berpindah dari ruang kerja ke rumah melalui perangkat pintar. Contoh yang paling sederhana adalah *smart home*, yaitu konsep ketika peralatan rumah tangga dikendalikan dari satu pusat, umumnya melalui aplikasi di *smartphone*, tablet, atau komputer, baik dari jarak dekat maupun jauh (Rita, 2024). Perangkat yang tampak sederhana pun tidak dapat dianggap aman. Perangkat yang tidak terlindungi dapat dimanfaatkan sebagai bagian dari *botnet* untuk melancarkan serangan seperti DDoS (Kumari & Jain, 2023).

Selain *smart home*, penerapan IoT mencakup pengendalian jarak jauh dan pemrosesan data melalui sensor canggih pada fasilitas umum, misalnya kamera CCTV jalan yang mendeteksi tindakan kriminal. Pada sektor pendidikan, IoT dipakai untuk mencatat kehadiran dan melacak siswa agar sekolah lebih aman, serta menjadikan sistem pendidikan konvensional lebih otomatis melalui kelas pintar yang interaktif (Saini & Saini, 2019). Pada sektor industri, sensor memproses data karyawan untuk meningkatkan efisiensi serta mengontrol kesehatan dan keselamatan kerja.

Seiring pertumbuhan tersebut, risiko peretasan tidak terelakkan karena konektivitas internet membuka peluang bagi peretas untuk mengeksploitasi kelemahan perangkat dan jaringan.

Celah penelitian. Kajian terdahulu cenderung menyoroti aspek keamanan IoT secara terpisah. Saini dan Saini (2019) menekankan pengelolaan pembaruan perangkat, Makhdoom dkk. (2019) membahas integritas perangkat lunak, Najib dkk. (2020) meninjau ancaman pada sisi tepi arsitektur IoT, Kumari dan Jain (2023) berfokus pada DDoS, sedangkan Javeed dkk. (2020) serta Serhat dkk. (2023) berfokus pada MitM. Dalam korpus yang dikaji, penulis tidak menemukan sintesis yang menghubungkan tantangan, jenis serangan, dan strategi mitigasi dalam satu kerangka. Akibatnya, pengelola jaringan sulit menentukan mitigasi yang harus didahulukan pada perangkat dengan sumber daya terbatas.

Tujuan dan kebaruan. Penelitian ini bertujuan (1) mengidentifikasi tantangan keamanan jaringan IoT, (2) menguraikan serangan DDoS dan MitM beserta strategi mitigasinya, dan (3) menyintesisnya menjadi kerangka yang dapat dipakai untuk menentukan prioritas. Kebaruan penelitian ini adalah (a) matriks pemetaan tantangan–serangan–mitigasi (Tabel 1), (b) penempatan enam strategi mitigasi pada lapisan arsitektur IoT berdasarkan model tujuh lapis (Najib dkk., 2020), dan (c) usulan prioritas mitigasi tiga tingkat (Tabel 2) yang mempertimbangkan cakupan perlindungan, beban terhadap perangkat, dan ketersediaan mitigasi pengganti. Usulan ini merupakan sintesis konseptual atas literatur dan belum diuji secara eksperimen.

TINJAUAN LITERATUR

1.1 Pengertian IoT

Internet of Things (IoT) adalah sistem yang terdiri atas perangkat, objek, dan mesin yang saling terhubung dan dapat mentransfer data melalui jaringan internet (Informatika Universitas Janabadra, n.d.). Istilah *things* merujuk pada berbagai perangkat yang dapat terhubung ke internet, seperti *smartphone*, mesin cuci, kendaraan, kamera keamanan, hingga alat kesehatan (Prasetyo, 2024). Menurut Informatika Universitas Janabadra (n.d.), setiap perangkat dalam ekosistem IoT dapat berkomunikasi, mengumpulkan data, menganalisis informasi yang diperoleh, dan bahkan bertindak secara otomatis berdasarkan data tersebut tanpa campur tangan manusia.

1.2 Penelitian Terdahulu

Penelitian terdahulu menyoroti aspek keamanan IoT yang berbeda. Saini dan Saini (2019) mengidentifikasi pengelolaan pembaruan perangkat sebagai tantangan signifikan. Jutaan perangkat IoT memerlukan pembaruan rutin untuk menjaga keamanan, tetapi tidak semuanya mendukung pembaruan *over-the-air* (OTA). Pengguna harus memperbarui secara manual, dan langkah ini berpotensi diabaikan sehingga menjadi celah keamanan.

Makhdoom dkk. (2019) menyimpulkan bahwa ancaman serius pada sistem IoT terletak pada integritas perangkat lunak, termasuk sistem operasi, aplikasi, dan konfigurasi perangkat. Ancaman terhadap integritas dapat membuka akses tidak sah dan manipulasi data yang membahayakan privasi serta kestabilan jaringan IoT.

Najib dkk. (2020) meninjau model arsitektur jaringan IoT tujuh lapis dan menekankan bahwa ancaman keamanan terutama terjadi pada sisi tepi (*edge side*), yaitu lapisan *edge nodes*, komunikasi, dan komputasi tepi (*edge computing*). Lapisan tersebut rentan karena menjadi titik pertama interaksi antara perangkat IoT dan jaringan maupun sistem *cloud* yang lebih besar.

Pada kelompok kajian yang berfokus pada jenis serangan, Kumari dan Jain (2023) mengkaji serangan DDoS pada jaringan IoT beserta langkah penanggulangannya. Javeed dkk. (2020) menganalisis serangan MitM, motivasi, dan pencegahannya, sedangkan Serhat dkk. (2023) menelaah serangan MitM pada protokol MQTT sebagai studi kasus. Ketiga kelompok kajian ini, yaitu pembaruan dan integritas, arsitektur, serta jenis serangan, berdiri sendiri. Hubungan antara tantangan, serangan, dan mitigasi belum disintesis dalam satu kerangka, dan inilah celah yang diisi penelitian ini.

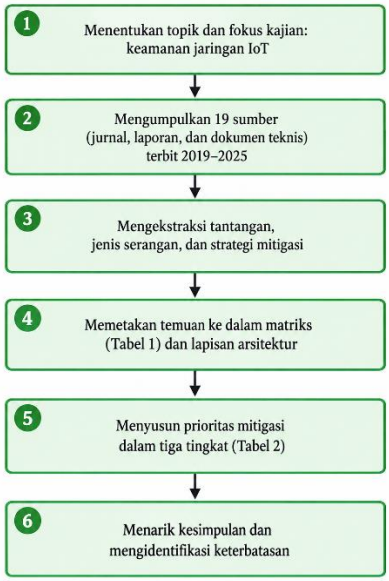
1.3 Sistem Keamanan Perangkat IoT

Keamanan perangkat IoT merupakan bagian integral dari strategi keamanan siber untuk melindungi perangkat terhubung dan jaringannya dari berbagai ancaman. Menurut Fortinet (n.d.), keamanan IoT mencakup upaya mengamankan perangkat keras, perangkat lunak, dan komunikasi data antarperangkat. Perangkat IoT sering berada dalam jaringan yang rentan karena keterbatasan sumber daya, standar keamanan yang tidak konsisten, dan kompleksitas arsitektur sistem. Oleh karena itu, strategi keamanan IoT perlu mencakup autentikasi yang kuat, enkripsi data, segmentasi jaringan, dan pemantauan lalu lintas secara terus-menerus agar serangan dapat terdeteksi dan dicegah sebelum berdampak lebih luas.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif berupa kajian literatur. Sumber dikumpulkan dari jurnal ilmiah, laporan industri, dan dokumen teknis daring yang membahas keamanan jaringan IoT dan terbit pada 2019–2025. Korpus yang dianalisis berjumlah 19 sumber, terdiri atas tujuh artikel jurnal ilmiah (Javeed dkk., 2020; Kumari & Jain, 2023; Makhdoom dkk., 2019; Najib dkk., 2020; Saini & Saini, 2019; Serhat dkk., 2023; Thilakarthne dkk., 2025), satu laporan ancaman industri (Yoachimik & Pacheco, 2025), dan sebelas dokumen teknis daring (Azura Team, 2024; Fortinet, n.d.; Informatika Universitas Janabadra, n.d.; Mei, 2024; Netmonk,

2019; Nexus Group, 2024; Olaes, 2025; Prasetyo, 2024; Rita, 2024; Sutisnawinata, 2023; Verizon, n.d.). Alur penelitian ditunjukkan pada Gambar 1.



Gambar 1. Alur Penelitian

Analisis dilakukan secara deskriptif dalam empat tahap. Pertama, tantangan, jenis serangan, dan strategi mitigasi diekstraksi dari setiap sumber. Kedua, ketiganya dipetakan ke dalam matriks, dengan tanda ● untuk perlindungan langsung yang dinyatakan sumber dan ○ untuk perlindungan tidak langsung yang merupakan sintesis penulis. Ketiga, setiap mitigasi ditempatkan pada lapisan arsitektur IoT berdasarkan model Najib dkk. (2020). Keempat, prioritas mitigasi ditentukan menurut tiga kriteria: cakupan perlindungan, beban terhadap perangkat, dan ketersediaan mitigasi pengganti. Data tren serangan DDoS disajikan secara deskriptif dari laporan Cloudflare (Yoachimik & Pacheco, 2025). Karena bersifat kajian literatur, penelitian ini tidak melakukan pengujian eksperimental.

HASIL DAN PEMBAHASAN

1.4 Tantangan Keamanan dalam Jaringan IoT

Keamanan jaringan IoT adalah perlindungan perangkat IoT dari serangan. Perangkat IoT kini ada di mana-mana, dan Statista memproyeksikan 75,44 miliar perangkat terpasang pada 2025, meningkat tajam dibanding tahun-tahun sebelumnya. Sebagian besar perangkat terhubung ke internet atau gateway melalui media nirkabel yang lebih lambat dan kurang aman, seperti 802.15.4, 802.11a/b/g/n/p, LoRa, ZigBee, NB-IoT, dan SigFox, sehingga sistem IoT rentan terhadap kebocoran data dan masalah privasi (Makhdoom dkk., 2019). Berdasarkan literatur, tantangan utama keamanan IoT adalah sebagai berikut.

a. Integritas Data
   Semakin banyak perangkat berada dalam ekosistem yang saling terhubung melalui IoT. Manipulasi pada satu titik data saja dapat berdampak pada seluruh data yang dipertukarkan antara sensor dan server utama (Saini & Saini, 2019).

b. **Risiko Autentikasi dan Enkripsi yang Lemah**
   Enkripsi dan autentikasi yang lemah mengancam keamanan perangkat IoT. Enkripsi yang memadai melindungi informasi sensitif, seperti data pelanggan, transaksi keuangan, dan

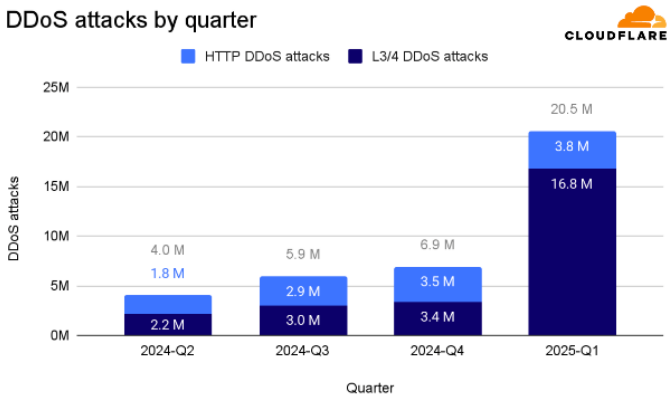
komunikasi internal, dari akses tidak sah karena hanya pihak berwenang yang dapat membaca data terenkripsi (Nexus Group, 2024). Perangkat yang tidak terenkripsi dengan baik dapat disadap, dan data yang dikirim dapat diubah atau dicuri sehingga informasi sensitif bocor. Di sisi lain, enkripsi membutuhkan daya pemrosesan, dan semakin kuat enkripsi semakin besar komputasi yang diperlukan (Verizon, n.d.).
Keamanan IoT juga bergantung pada autentikasi. Autentikasi yang lemah, misalnya kata sandi bawaan atau PIN sederhana, memudahkan peretas mengakses perangkat sehingga terjadi pencurian data, pengendalian perangkat tanpa izin, dan intrusi jaringan yang lebih luas. Perangkat yang tidak terlindungi juga dapat menjadi bagian dari *botnet*, yaitu jaringan perangkat yang diretas untuk melancarkan serangan siber seperti DDoS.

c. Segmentasi Jaringan Kurang Memadai
Segmentasi jaringan yang buruk memungkinkan penyerang bergerak secara lateral setelah menembus satu sistem. Tanpa pemisahan antara lingkungan IT, OT, dan IoT, perangkat IoT yang disusupi, misalnya termostat pintar, dapat membuka akses ke sistem kontrol industri atau data sensitif (Olaes, 2025).

d. Pembaruan
Tidak semua perangkat mendukung pembaruan otomatis, sehingga pembaruan harus dilakukan secara manual dan berpotensi terabaikan. Investasi keamanan pada infrastruktur dan jaringan harus menjadi prioritas, karena IoT melibatkan jutaan titik data dan setiap titik harus diamankan (Saini & Saini, 2019).

1.5 Jenis Serangan Perangkat IoT

a. Serangan *Distributed Denial of Service* (DDoS)
Menurut Kumari dan Jain (2023), serangan DDoS merupakan salah satu serangan jaringan IoT yang paling umum dan menjadi masalah serius bagi konsultan TI dan profesional keamanan. DDoS mengganggu sumber daya jaringan dengan membanjiri lalu lintas komunikasi menggunakan permintaan bertubi-tubi, sehingga server melambat dan tidak dapat melayani pengguna atau server lain. Serangan ini sulit dicegah dan dideteksi karena dilancarkan dari banyak lokasi dan perangkat yang berbeda (Kumari & Jain, 2023).
Seiring pesatnya penggunaan IoT, serangan DDoS meningkat tajam. Laporan Cloudflare (Yoachimik & Pacheco, 2025) mencatat 20,5 juta serangan DDoS pada kuartal pertama 2025, naik 358% dibanding periode yang sama pada tahun sebelumnya. Gambar 2 memperlihatkan lonjakan dari 6,9 juta serangan pada kuartal keempat 2024 menjadi 20,5 juta serangan pada kuartal pertama 2025, yang terdiri atas 16,8 juta serangan L3/4 dan 3,8 juta serangan HTTP. Angka tersebut mencakup seluruh target serangan dan tidak khusus perangkat IoT, sehingga hanya dipakai sebagai indikator tren ancaman DDoS secara umum.



Gambar 2. Diagram Peningkatan serangan DDoS
Sumber: *Cloudflare*

b. Serangan *Man in the Middle*
Serangan MitM melibatkan dua pihak yang berkomunikasi dan penyerang sebagai pihak ketiga yang menyusup di antara keduanya tanpa disadari korban (Javeed dkk., 2020). Menurut Serhat dkk. (2023), serangan MitM terjadi ketika penyerang berada pada jaringan yang sama dengan perangkat target. Javeed dkk. (2020) menyatakan serangan ini dapat diarahkan ke berbagai jalur komunikasi, yaitu GSM, *Wi-Fi*, UMTS, dan Bluetooth, sehingga data yang mengalir di antara titik akhir dapat disadap atau diubah. Tujuannya adalah mencuri data dan informasi pribadi yang sedang ditransmisikan untuk disalahgunakan. Pada bentuk pasif, penyerang hanya menyadap komunikasi, sedangkan pada bentuk aktif penyerang dapat mengubah data sehingga integritas data terancam.

1.6 Teknik Pencegahan

Berdasarkan ancaman yang diuraikan di atas, enam langkah pencegahan berikut dapat diterapkan untuk melindungi sistem IoT dari peretasan.

1. Menggunakan *Firewall* dan Sistem Deteksi Intrusi (IDS)
   Firewall memblokir lalu lintas yang mencurigakan, sedangkan IDS membantu mendeteksi pola serangan sedini mungkin. Keduanya dapat dipakai untuk melindungi perangkat dari serangan DDoS (Mei, 2024).
2. Menggunakan Enkripsi *End-to-End*
   Komunikasi antarperangkat IoT dilindungi dengan protokol seperti TLS atau VPN untuk mengurangi risiko serangan MitM (Serhat dkk., 2023; Sutisnawinata, 2023). Karena enkripsi membutuhkan daya komputasi (Verizon, n.d.), pemilihan metode enkripsi perlu disesuaikan dengan kemampuan perangkat.
3. Mengaktifkan Autentikasi Dua Faktor (2FA)
   Autentikasi dua faktor menambahkan lapisan perlindungan ekstra pada akses ke perangkat IoT (Sutisnawinata, 2023).
4. Membatasi Lalu Lintas dan *Rate Limiting*
   Pembatasan jumlah permintaan yang dapat diterima perangkat IoT mencegah banjir lalu lintas akibat serangan DDoS (Azura Team, 2024).
5. Menggunakan Jaringan Tersegmentasi
   Memisahkan perangkat IoT dari jaringan utama mengurangi dampak serangan apabila satu perangkat berhasil disusupi (Mei, 2024).
6. Pembaruan *Firmware* dan Perangkat Lunak
   Perangkat IoT perlu selalu menggunakan versi terbaru untuk menutup celah peretasan (Azura Team, 2024). Karena tidak semua perangkat mendukung pembaruan OTA (Saini & Saini, 2019), pembaruan manual perlu dijadwalkan agar tidak terabaikan.

1.7 Pemetaan Tantangan, Serangan, dan Mitigasi

Tabel 1 memetakan enam strategi mitigasi terhadap empat tantangan dan dua jenis serangan yang telah diuraikan. Pemetaan ini merupakan sintesis penulis atas sumber yang dikaji.

Tabel 1. Matriks pemetaan strategi mitigasi terhadap tantangan dan serangan IoT

Strategi mitigasi	Integritas data	Autentikasi & enkripsi	Segmentasi	Pembaruan	DDoS	MitM
***Firewall* dan IDS (Mei, 2024)**	–	–	○	–	●	○
Enkripsi *end-to-end* (TLS/VPN) (Serhat dkk., 2023; Sutisnawinata, 2023)	●	●	–	–	–	●

Strategi mitigasi	Integritas data	Autentikasi & enkripsi	Segmentasi	Pembaruan	DDoS	MitM
Autentikasi dua faktor (Sutisnawinata, 2023)	○	●	–	–	○	–
***Rate limiting* (Azura Team, 2024)**	–	–	–	–	●	–
Segmentasi jaringan (Mei, 2024)	–	–	●	–	○	○
Pembaruan *firmware* (Azura Team, 2024)	○	–	–	●	○	–

Keterangan: ● perlindungan langsung (dinyatakan sumber); ○ perlindungan tidak langsung (sintesis penulis); – tidak relevan. Kolom Integritas data hingga Pembaruan adalah tantangan; kolom DDoS dan MitM adalah serangan.

Matriks ini menghasilkan dua temuan. Pertama, setiap tantangan dan serangan memiliki setidaknya satu mitigasi langsung. Kedua, MitM dan integritas data hanya bergantung pada satu mitigasi langsung, yaitu enkripsi, sedangkan DDoS memiliki dua mitigasi langsung (*firewall*/IDS dan *rate limiting*) sehingga lebih tahan terhadap kegagalan satu kontrol. Ketergantungan pada enkripsi ini menjadi persoalan karena enkripsi membutuhkan daya komputasi (Verizon, n.d.) yang terbatas pada banyak perangkat IoT.

1.8 Penempatan pada Lapisan Arsitektur dan Prioritas Mitigasi

Menggunakan model arsitektur tujuh lapis (Najib dkk., 2020) yang menempatkan ancaman terutama pada sisi tepi, setiap mitigasi ditempatkan pada lapisan *edge nodes*, komunikasi, atau komputasi tepi. Lapisan di atasnya (akumulasi data hingga aplikasi) berada di luar cakupan kajian ini. Berdasarkan pemetaan pada Tabel 1 dan penempatan lapisan tersebut, diusulkan prioritas tiga tingkat pada Tabel 2.

Tabel 2. Usulan prioritas mitigasi tiga tingkat dan penempatannya pada lapisan arsitektur IoT

Tingkat	Strategi mitigasi	Lapisan	Dasar penentuan prioritas
1. Langkah dasar	Pembaruan *firmware*; autentikasi dua faktor dan penggantian kredensial bawaan; segmentasi jaringan	*Edge nodes* (pembaruan, autentikasi); komunikasi (segmentasi)	Masing-masing menyentuh tiga sasaran pada Tabel 1 (● dan ○), menutup akar masalah (celah, kredensial lemah, pergerakan lateral), dan tidak menambah beban komputasi berat pada perangkat.
2. Perlindungan komunikasi	Enkripsi *end-to-end* (TLS/VPN)	Komunikasi	Satu-satunya mitigasi langsung untuk MitM dan integritas data (tidak ada pengganti), tetapi membutuhkan komputasi (Verizon, n.d.), sehingga diterapkan sesuai kemampuan perangkat.
3. Deteksi dan pembatasan	*Firewall* dan IDS; *rate limiting*	Komputasi tepi (*gateway*)	Khusus DDoS dan saling melengkapi (dua mitigasi langsung), dijalankan di *gateway* sehingga tidak membebani perangkat; berfungsi sebagai lapisan tambahan.

Urutan ini mengikuti tiga kriteria. Langkah dasar didahulukan karena cakupannya luas dan bebannya ringan. Enkripsi ditempatkan pada tingkat kedua karena tidak memiliki pengganti, tetapi implementasinya perlu disesuaikan dengan kemampuan perangkat. Firewall, IDS, dan *rate limiting* ditempatkan pada tingkat ketiga karena saling melengkapi sehingga penerapannya dapat bertahap. Urutan ini merupakan usulan konseptual dan belum divalidasi secara eksperimental.

1.9 Kebaruan dan Implikasi

Dibandingkan kajian terdahulu yang berfokus pada pembaruan (Saini & Saini, 2019), integritas perangkat lunak (Makhdoom dkk., 2019), ancaman per lapisan (Najib dkk., 2020), DDoS (Kumari & Jain, 2023), dan MitM (Javeed dkk., 2020; Serhat dkk., 2023), penelitian ini memberikan tiga kontribusi. Pertama, matriks pemetaan tantangan–serangan–mitigasi (Tabel 1)

menyatukan pembahasan yang semula terpisah dan menampakkan ketergantungan MitM pada enkripsi sebagai satu-satunya mitigasi langsung. Kedua, penempatan mitigasi pada lapisan arsitektur (Najib dkk., 2020) menunjukkan bahwa kontrol dasar bekerja pada *edge nodes* dan jaringan, sedangkan kontrol DDoS dapat dijalankan di *gateway*. Ketiga, prioritas tiga tingkat (Tabel 2) menerjemahkan temuan literatur menjadi urutan penerapan yang mempertimbangkan keterbatasan sumber daya perangkat.

Secara praktis, pengelola jaringan skala kecil, seperti rumah, kampus, atau usaha kecil, dapat memulai dari Tingkat 1 tanpa investasi besar, lalu menambah enkripsi dan kontrol DDoS sesuai kapabilitas perangkat.

KESIMPULAN

Penelitian ini mengidentifikasi empat tantangan keamanan jaringan IoT, yaitu integritas data, autentikasi dan enkripsi yang lemah, segmentasi jaringan yang kurang memadai, serta pembaruan perangkat yang diabaikan. Tantangan tersebut dieksploitasi terutama melalui serangan DDoS dan MitM. Beberapa perangkat IoT tidak aman dan vendornya mungkin tidak menyediakan pembaruan *firmware*, sehingga perangkat rentan diretas. Enam strategi mitigasi dipetakan terhadap tantangan dan serangan tersebut, yaitu *firewall* dan IDS, enkripsi *end-to-end*, autentikasi dua faktor, *rate limiting*, segmentasi jaringan, dan pembaruan *firmware*.

Kebaruan penelitian ini terletak pada pemetaan terintegrasi tantangan–serangan–mitigasi, penempatan mitigasi pada lapisan arsitektur IoT, dan prioritas mitigasi tiga tingkat. Hasilnya menunjukkan bahwa MitM hanya memiliki satu mitigasi langsung sehingga langkah dasar, yaitu pembaruan *firmware*, autentikasi, dan segmentasi, diusulkan didahulukan, disusul enkripsi sesuai kemampuan perangkat, lalu *firewall*, IDS, dan *rate limiting*. Segmentasi, yaitu memisahkan perangkat IoT dari jaringan utama, merupakan salah satu langkah paling sederhana untuk mengurangi dampak serangan.

Penelitian ini memiliki keterbatasan. Korpus berjumlah 19 sumber dan sebelas di antaranya adalah dokumen teknis daring, pemetaan ○ merupakan sintesis penulis, dan prioritas tiga tingkat belum diuji secara eksperimen. Penelitian lanjutan disarankan menguji kerangka ini pada *testbed* IoT, misalnya dengan simulasi DDoS dan MitM pada protokol MQTT, serta mengukur beban komputasi enkripsi pada perangkat dengan sumber daya terbatas.

DAFTAR PUSTAKA

Azura Team. (2024, 21 Oktober). *Mendeteksi dan mencegah serangan DDoS pada jaringan IoT*. Azura Labs. https://azuralabs.id/blog-security-testing/mendeteksi-dan-mencegah-serangan-ddos-pada-jaringan-iot

Fortinet. (n.d.). *Apa itu keamanan IoT? Tantangan dan persyaratan*.

Informatika Universitas Janabadra. (n.d.). *Konsep dasar Internet of Things: Mengenal jaringan terhubung yang membawa perubahan*. https://informatika.janabadra.ac.id/konsep-dasar-internet-of-things-iot-mengenal-jaringan-terhubung-yang-membawa-perubahan/

Javeed, D., Badamasi, U. M., Ndubuisi, C. O., Soomro, F., & Asif, M. (2020). Man in the middle attacks: Analysis, motivation and prevention. *[nama jurnal]*, *8*(7), 52–58. https://doi.org/10.13140/RG.2.2.22752.81928

Kumari, P., & Jain, A. K. (2023). A comprehensive study of DDoS attacks over IoT network and their countermeasures. *Computers & Security, 127*, Article 103096. https://doi.org/10.1016/j.cose.2023.103096

Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P., & Ni, W. (2019). Anatomy of threats to the Internet of Things. *IEEE Communications Surveys & Tutorials, 21*(2).

Mei. (2024, 4 Juli). *Mengidentifikasi dan mencegah serangan DDoS pada perangkat IoT*. Nusabot. https://nusabot.id/blog/mengidentifikasi-dan-mencegah-serangan-ddos-pada-perangkat-iot/

Najib, W., Sulistyo, S., & Widyawan. (2020). Tinjauan ancaman dan solusi keamanan pada teknologi Internet of Things. *Jurnal Nasional Teknik Elektro dan Teknologi Informasi, 9*(4).

Netmonk. (2019, 13 Juni). *Internet of Things (IoT)*. [URL]

Nexus Group. (2024, 28 Maret). *What are the security challenges of IoT?* https://www.nexusgroup.com/what-are-the-security-challenges-of-iot/

Olaes, T. (2025, 1 Mei). *Top IT, and IoT security challenges and best practices*. Balbix. https://www.balbix.com/insights/addressing-iot-security-challenges/

Prasetyo, I. (2024, 30 Oktober). *Apa itu Internet of Things? Pengertian, cara kerja, dan contohnya*. Telkom University. https://docif.telkomuniversity.ac.id/apa-itu-iot/

Rita, P. S. (2024, Agustus). *Penerapan IoT dalam smart home dan manfaatnya*. Cloud Computing Indonesia. https://www.cloudcomputing.id/pengetahuan-dasar/penerapan-iot-smar-thome

Saini, M. K., & Saini, R. K. (2019). Internet of Things (IoT) applications and security challenges: A review. *International Journal of Engineering Research & Technology, 7*(12).

Serhat, C., Nesibe, Y., & Semih, C. (2023). MitM attacks and IoT security: A case study on MQTT. *[nama jurnal], 3*(2), 99–106.

Sutisnawinata, K. (2023, 14 November). *Man in the middle attack: Arti, cara kerja, pencegahan*. ASDF.ID. https://www.asdf.id/man-in-the-middle-attack-adalah/

Thilakarthne, N. N., Abu Bakar, M. S., Abas, H. E., & Yassin, H. (2025). Internet of things enabled smart agriculture: Current status, latest advancements, challenges and countermeasures. *[nama jurnal]*.

Verizon. (n.d.). *IoT security: Why you need to encrypt your data*. https://www-verizon-com.translate.goog/business/resources/articles/s/iot-security-why-you-need-to-encrypt-your-data

Yoachimik, O., & Pacheco, J. (2025, 27 April). *Targeted by 20.5 million DDoS attacks, up 358% year-over-year: Cloudflare's 2025 Q1 DDoS threat report*. Cloudflare.