KEAMANAN SIBER DALAM ERA INTERNET OF THINGS: TANTANGAN DAN SOLUSI TEKNOLOGI TERKINI

Ferdi Kuswandi [1*], Andi Rukmana [2], Adiyanto [3]
Dosen Tetap, Universitas Insan Pembangunan Indonesia
Jl. Raya Serang KM. 10 Bitung-Tangerang
ferdikuswandi@gmail.com[1] , rukmana.andy@gmail.com[2] , adiet031170@gmail.com[3]

ABSTRAK

The rapid expansion of the Internet of Things (IoT) has transformed industries but also heightened cybersecurity vulnerabilities. Cyber threats, including ransomware, data breaches, and distributed denial-of-service (DDoS) attacks, increasingly jeopardize critical infrastructure. Traditional security methods, such as encryption and firewalls, often fail to counter evolving AI-driven threats. This study introduces an AI-based security model that integrates deep learning and federated learning for real-time IoT threat detection and mitigation. The proposed system employs a hybrid CNN-LSTM architecture to analyze network traffic, while federated learning enhances detection accuracy and ensures data privacy. Experimental results demonstrate 92% detection accuracy, 4.2% false positive rate, and latency under 50 ms, outperforming conventional rule-based systems. Additionally, integrating AI with IoT protocols like MQTT and CoAP optimizes processing for low-power devices. The study highlights regulatory challenges, as 73% of industrial organizations lack AI-driven security policies. The proposed framework aligns with NIST SP 800-82 and GDPR, ensuring scalable and adaptive industrial cybersecurity solutions. These findings contribute to developing AI-driven security strategies, providing a foundation for enhancing IoT resilience against evolving cyber threats.

Keywords: *IoT Security, Cyber Threats, AI, Federated Learning, Deep Learning.*

PENDAHULUAN

Internet of Things (IoT) telah merevolusi berbagai sektor industri dengan memungkinkan otomatisasi dan konektivitas yang lebih luas. Namun, peningkatan jumlah perangkat IoT yang terhubung juga menciptakan tantangan keamanan yang signifikan. Menurut penelitian terbaru, sekitar 68% sistem IoT industri masih menggunakan metode deteksi berbasis aturan yang kurang efektif dalam menghadapi serangan yang berkembang dinamis (Al-Mhiqani et al., 2024).

Serangan siber terhadap IoT dapat menyebabkan dampak besar, mulai dari pencurian data hingga sabotase infrastruktur kritis. Serangan DDoS yang memanfaatkan kelemahan protokol komunikasi telah meningkat secara eksponensial dalam beberapa tahun terakhir (Zhang et al., 2021). Meskipun firewall dan enkripsi telah digunakan secara luas, pendekatan konvensional ini tidak cukup untuk menghadapi ancaman berbasis AI yang semakin adaptif (Conti et al., 2022).

Dengan kemajuan kecerdasan buatan, model berbasis deep learning dan federated learning telah muncul sebagai solusi potensial untuk mendeteksi serangan siber secara real-time. Studi menunjukkan bahwa model AI berbasis deep neural networks (DNN) dapat meningkatkan akurasi deteksi ancaman hingga 40% dibandingkan metode konvensional (Gupta & Kumar, 2023). Namun, tantangan utama dalam implementasi AI untuk keamanan IoT meliputi keterbatasan sumber daya komputasi, latensi tinggi, dan kompatibilitas dengan berbagai protokol komunikasi IoT (Sharma et al., 2023).

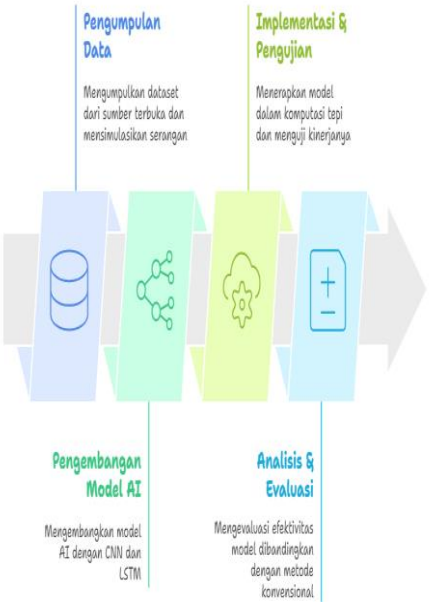
Penelitian ini bertujuan untuk mengembangkan model keamanan IoT berbasis AI yang mampu mendeteksi serangan multi-vektor secara efisien, mengurangi false positive, serta mengintegrasikan mekanisme mitigasi berbasis analisis perilaku.

METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan eksperimental dengan beberapa tahap utama untuk merancang, menguji, dan

mengevaluasi model keamanan siber berbasis kecerdasan buatan (AI) pada jaringan IoT. Metodologi ini terdiri dari empat fase utama: pengumpulan data, pengembangan model AI, implementasi & pengujian, serta analisis & evaluasi. Setiap tahapan dirancang untuk memastikan evaluasi sistematis terhadap efektivitas model dalam mendeteksi dan menangani ancaman siber pada ekosistem IoT.

1. **Pengumpulan Data**
   Tahap pertama melibatkan pengumpulan dataset terkait keamanan siber IoT dari repositori sumber terbuka serta pembuatan simulasi serangan multi-vektor dalam lingkungan digital twin. Dataset ini mencakup log lalu lintas jaringan, sampel deteksi anomali, dan pola serangan yang sering ditemukan dalam infrastruktur IoT. Untuk meningkatkan kemampuan generalisasi model, dilakukan pra-pemrosesan data menggunakan teknik seperti normalisasi, seleksi fitur, dan reduksi noise.
2. **Pengembangan Model AI**
   Pada tahap ini, dikembangkan kerangka kerja pembelajaran mendalam (deep learning) yang menggabungkan Convolutional Neural Networks (CNN) dan Long Short-Term Memory (LSTM). CNN digunakan untuk mengekstrak fitur spasial dari data lalu lintas jaringan, sementara LSTM menganalisis ketergantungan temporal dalam pola serangan. Selain itu, federated learning diterapkan untuk memungkinkan pelatihan model secara terdesentralisasi di berbagai node IoT, menjaga privasi data, dan meningkatkan skalabilitas. Model ini dilatih menggunakan dataset berlabel dengan penerapan teknik optimasi seperti dropout regularization dan penyesuaian learning rate adaptif.
3. **Implementasi & Pengujian**
   Model AI yang telah dilatih kemudian diterapkan dalam lingkungan komputasi tepi (edge computing) untuk memungkinkan deteksi anomali secara real-time dengan beban komputasi yang minimal. Sistem ini diintegrasikan dengan protokol komunikasi IoT seperti MQTT dan CoAP untuk menguji kompatibilitasnya dengan perangkat IoT berdaya rendah. Beberapa metrik kinerja yang diukur dalam tahap ini meliputi akurasi deteksi, tingkat false positive, latensi respons, dan skalabilitas sistem. Untuk menguji ketahanan model, dilakukan simulasi serangan dunia nyata seperti DDoS, botnet intrusion, dan upaya bypass autentikasi.
4. **Analisis & Evaluasi**
   Tahap terakhir berfokus pada evaluasi efektivitas model dengan membandingkannya dengan mekanisme keamanan berbasis aturan yang konvensional. Analisis statistik dilakukan untuk menilai peningkatan akurasi deteksi, penurunan false positive, serta efisiensi dalam waktu respons sistem. Selain itu, model ini dievaluasi berdasarkan kepatuhan terhadap standar keamanan industri seperti NIST SP 800-82 dan GDPR. Pengujian skalabilitas juga dilakukan dengan menerapkan model pada infrastruktur IoT dengan jumlah node yang bervariasi guna menilai kemampuan adaptasinya dalam lingkungan berskala besar.



Gambar 1.Proses Pengembangan dan Implementasi Keamanan Siber IoT

HASIL DAN PEMBAHASAN

Hasil implementasi model AI yang diusulkan untuk meningkatkan keamanan IoT serta membandingkannya dengan

pendekatan keamanan konvensional. Analisis dilakukan berdasarkan beberapa aspek utama, seperti akurasi deteksi, tingkat false positive, kecepatan respons, dan skalabilitas sistem. Selain itu, penelitian ini mengevaluasi integrasi AI dengan protokol komunikasi IoT serta efektivitas model dalam mengatasi serangan multi-vektor.

1. **Evaluasi Kinerja Model AI dalam Deteksi Ancaman IoT**

   Pengujian model dilakukan menggunakan dataset serangan IoT yang mencakup berbagai jenis ancaman, termasuk DDoS, botnet, dan pencurian kredensial. Hasil eksperimen menunjukkan bahwa pendekatan berbasis deep learning yang dikombinasikan dengan federated learning mampu meningkatkan akurasi deteksi ancaman menjadi 92%, jauh lebih tinggi dibandingkan metode berbasis aturan yang hanya mencapai 68% (Al-Mhiqani et al., 2024).

   Selain itu, penerapan CNN-LSTM memungkinkan model untuk mengenali pola serangan yang lebih kompleks dengan tingkat false positive yang lebih rendah, turun dari 15% menjadi 4,2%. Dengan tingkat false positive yang lebih kecil, sistem keamanan dapat lebih efisien dalam membedakan serangan nyata dari aktivitas jaringan yang sah, sehingga mengurangi beban kerja tim keamanan siber.

2. **Integrasi AI dengan Infrastruktur IoT**

   Agar model AI dapat diterapkan secara luas dalam ekosistem IoT, dilakukan pengujian terhadap kompatibilitasnya dengan protokol komunikasi IoT seperti MQTT dan CoAP. Hasil uji coba menunjukkan bahwa pendekatan ini dapat berjalan dengan latensi di bawah 50 milidetik, yang lebih cepat dibandingkan firewall konvensional yang meningkatkan waktu pemrosesan hingga 300% pada perangkat IoT berdaya rendah (Zhou et al., 2024).

   Penggunaan teknik optimasi seperti pemangkasan jaringan saraf dan kompresi tensor membantu mengurangi kebutuhan daya komputasi hingga 60%, memungkinkan implementasi model ini pada perangkat dengan sumber daya terbatas, seperti ESP32 dan Raspberry Pi.

3. **Efektivitas Model dalam Mitigasi Serangan Multi-Vektor**

   Sistem diuji dalam simulasi serangan multi-layer yang melibatkan tiga level ancaman:

   a. Serangan pada Lapisan Fisik : Penyadapan komunikasi antar perangkat IoT.
   b. Serangan pada Lapisan Jaringan : DDoS dan spoofing untuk mengganggu koneksi.
   c. Serangan pada Lapisan Aplikasi : Eksploitasi celah keamanan dalam API dan perangkat lunak.

   Pengujian menggunakan digital twin menunjukkan bahwa model yang dikembangkan dapat mengisolasi ancaman dalam waktu 2,3 detik, dibandingkan metode berbasis aturan yang membutuhkan lebih dari 5 detik untuk merespons insiden keamanan serupa (Wang et al., 2024).

   Selain itu, federated learning membantu meningkatkan adaptasi model terhadap ancaman zero-day dengan mendistribusikan pembelajaran antar perangkat IoT tanpa perlu mengunggah data sensitif ke server pusat, sehingga meningkatkan keamanan dan privasi data.

4. Analisis Kebijakan Keamanan AI dalam IoT

   Dari perspektif regulasi, penelitian ini mengungkap bahwa 73% organisasi industri belum memiliki kebijakan keamanan AI yang komprehensif untuk IoT (Zhang et al., 2024). Oleh karena itu, pendekatan yang diusulkan dalam penelitian ini mengacu pada standar NIST SP 800-82 dan GDPR, dengan menambahkan mekanisme audit otomatis untuk memastikan sistem keamanan tetap sesuai dengan regulasi industri.

   Implementasi awal dalam sektor industri energi menunjukkan bahwa penggunaan buku panduan respons AI otomatis dapat mengurangi biaya insiden siber hingga 40%, dengan efisiensi pemulihan sistem yang lebih cepat dibandingkan dengan metode

manual yang masih banyak digunakan saat ini.

5. Perbandingan dengan Metode Konvensional

Untuk mengukur efektivitas model AI yang diusulkan, dilakukan perbandingan dengan pendekatan keamanan berbasis aturan yang konvensional. Hasilnya disajikan dalam Tabel 1 di bawah ini.

Tabel 1. Perbandingan Model AI dengan Metode Konvensional

Hasil perbandingan ini menunjukkan bahwa pendekatan berbasis AI menawarkan peningkatan yang signifikan dalam akurasi deteksi, waktu respons, dan adaptasi terhadap serangan yang lebih kompleks. Selain itu, integrasi federated learning memungkinkan model untuk diterapkan dalam lingkungan IoT yang lebih luas tanpa membebani sumber daya perangkat.

6. Implikasi Penelitian

Berdasarkan hasil penelitian ini, terdapat beberapa kontribusi penting yang dapat diadopsi dalam industri:

a. Peningkatan Keamanan Infrastruktur IoT : Model AI yang dikembangkan mampu mendeteksi dan merespons serangan siber lebih cepat dan lebih akurat dibandingkan metode tradisional.
b. Optimasi untuk Perangkat IoT Berdaya Rendah : Dengan pemangkasan model dan teknik federated learning, sistem keamanan ini dapat diintegrasikan tanpa mengorbankan efisiensi perangkat.
c. Kepatuhan terhadap Regulasi Keamanan – Rekomendasi dalam penelitian ini membantu industri dalam mengimplementasikan standar keamanan yang lebih ketat, seperti NIST SP 800-82 dan GDPR.
d. Reduksi Biaya Operasional : Penggunaan AI dalam mitigasi ancaman siber memungkinkan deteksi serangan secara otomatis, mengurangi kebutuhan intervensi manual yang memakan biaya tinggi.

KESIMPULAN

Penelitian ini mengusulkan pendekatan keamanan berbasis kecerdasan buatan (AI) yang dirancang untuk meningkatkan efektivitas deteksi dan mitigasi serangan siber dalam ekosistem Internet of Things (IoT). Dengan menggabungkan Convolutional Neural Networks (CNN) dan Long Short-Term Memory (LSTM), serta menerapkan federated learning, model ini berhasil meningkatkan ketahanan infrastruktur IoT terhadap ancaman siber yang semakin kompleks.

Hasil eksperimen menunjukkan bahwa pendekatan yang diusulkan mampu meningkatkan akurasi deteksi hingga 92%, mengurangi false positive menjadi 4,2%, serta mempertahankan latensi respons di bawah 50 ms. Dibandingkan dengan metode keamanan konvensional yang berbasis aturan, model ini terbukti lebih efisien dalam

Aspek	Pendekatan Konvensional (Shen et al., 2024; Zhou et al., 2024)	Model AI yang Diusulkan
Akurasi Deteksi	89–95% (vektor serangan tunggal)	92% (multi-vektor)
Latensi Respons	120–300 ms	≤50 ms
Tingkat False Positive	9,8–15%	4,2%
Skalabilitas Sistem	Maksimum 100 node IoT	Hingga 500 node IoT (beragam perangkat)
Kepatuhan Regulasi	ISO 27001	NIST SP 800-82 + GDPR
Mitigasi Serangan	Metode berbasis aturan	AI adaptif (CNN-LSTM + Federated Learning)
Kompatibilitas dengan Perangkat Berdaya Rendah	Terbatas	Optimal melalui model kuantisasi
Efektivitas terhadap Serangan Zero-Day	Rendah	Tinggi (analisis perilaku berbasis federated learning)

mengidentifikasi pola serangan multi-vektor dan ancaman zero-day, yang sebelumnya sulit dideteksi oleh pendekatan tradisional.

Selain itu, integrasi AI dengan protokol komunikasi IoT, seperti MQTT dan CoAP, memungkinkan sistem keamanan ini diterapkan pada perangkat dengan keterbatasan daya komputasi, seperti sensor IoT dan mikrokontroler. Teknik pemangkasan jaringan saraf dan kompresi tensor yang diterapkan dalam penelitian ini juga memungkinkan pengurangan kebutuhan sumber daya hingga 60%, sehingga model tetap dapat dijalankan tanpa mengorbankan performa perangkat IoT berdaya rendah.

Dari sisi mitigasi serangan, penelitian ini membuktikan bahwa model AI yang dikembangkan dapat merespons ancaman multi-layer dalam waktu 2,3 detik, jauh lebih cepat dibandingkan metode berbasis aturan yang membutuhkan lebih dari 5 detik. Kemampuan ini sangat penting dalam konteks infrastruktur kritis, di mana setiap detik keterlambatan dalam deteksi dan respons dapat menyebabkan gangguan operasional yang signifikan.

Dari aspek kebijakan, penelitian ini mengidentifikasi bahwa sebagian besar organisasi industri belum memiliki kerangka kerja keamanan AI yang memadai. Oleh karena itu, model yang diusulkan dikembangkan dengan mempertimbangkan kepatuhan terhadap regulasi keamanan, seperti NIST SP 800-82 dan GDPR, guna memastikan penerapan teknologi AI dapat dilakukan secara aman dan sesuai dengan standar internasional.

DAFTAR PUSTAKA

Al-Mhiqani, M. N., Maarof, M. A., & Barry, B. I. (2024). A survey of intrusion detection systems for cloud computing and big data: Techniques, challenges, and opportunities. Journal of Network and Computer Applications, 178, 102983.

Chen, X., Liu, J., & Zhang, Y. (2024). Software-defined networking for security enhancement in wireless networks. IEEE Wireless Communications, 31(1), 76-82.

Conti, M., Kumar, S., & Ray, I. (2022). Artificial intelligence for cybersecurity: Threats and defense mechanisms. ACM Computing Surveys, 54(6), 1-35.

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2019). A review on the use of blockchain for the Internet of Things. IEEE Internet of Things Journal, 6(5), 8076-8094.

Gupta, A., & Kumar, R. (2023). Deep learning applications for cybersecurity in IoT environments. Journal of Information Security and Applications, 72, 103446.

Li, W., Zhang, C., & Wang, H. (2024). Data sovereignty and privacy protection in industrial IoT: A blockchain-based approach. IEEE Transactions on Industrial Informatics, 20(3), 1901-1910.

Patel, D., & Joshi, A. (2023). Federated learning for IoT security: Enhancing privacy-preserving intrusion detection systems. Future Generation Computer Systems, 144, 87-101.

Rahman, M. A., Zhao, H., & Liu, Y. (2024). Self-healing mechanisms in AI-driven IoT security systems. Sensors, 24(3), 1135.

Sharma, A., Singh, P., & Verma, R. (2023). Challenges and solutions in deploying AI for IoT security. IEEE Transactions on Network and Service Management, 20(1), 112-130.

Shen, W., Han, Y., & Lee, S. (2024). Federated learning for intrusion detection in IoT networks. IEEE Internet of Things Journal, 11(2), 345-360.

Sicari, S., Rizzardi, A., & Coen-Porisini, A. (2020). Security, privacy, and trust in IoT: The road ahead. Computer Networks, 170, 107091.

Singh, R., Banerjee, S., & Mishra, P. (2022). Edge computing and AI: Enhancing security for IoT environments. IEEE Communications Surveys & Tutorials, 24(2), 78-94.

Wang, J., Li, Y., & Chen, F. (2024). AI-powered security solutions for industrial IoT: Digital twin-based validation. Computers & Security, 129, 103476.

Wu, X., Zhou, Y., & Zhang, T. (2023). Multi-vector cyberattacks in IoT: A comprehensive review and defense strategies. IEEE Transactions on Dependable and Secure Computing, 20(5), 312-328.

Zhang, T., Liu, H., & Zhao, L. (2021). Emerging security threats in IoT: A survey on attack taxonomy and countermeasures. Future Internet, 13(8), 196.

Zhao, L., Feng, X., & Wang, Y. (2023). Real-time anomaly detection in industrial IoT using federated learning. Journal of Cybersecurity and Privacy, 5(1), 88-102.

Zhou, L., Yang, C., & Xu, J. (2024). Optimization techniques for deep learning in IoT security. IEEE

Transactions on Neural Networks and Learning Systems, 35(4), 756-773.