
2025
7 – 13 April 2025
Kamsib Indonesia on Paper
Edisi 10
Tetap Aman Bersama Kamsib
Kamsib Indonesia on Paper adalah majalah yang membahas berbagai aspek keamanan siber, mulai dari ancaman terbaru, teknik perlindungan, hingga tren teknologi yang memengaruhi lanskap keamanan digital.

# Kamsib Indonesia on Paper

**Edisi 10**
**7 – 13 April 2025**

*Tujuannya adalah membuat layanan tersebut menjadi lambat, tidak stabil, atau bahkan sepenuhnya tidak dapat diakses oleh pengguna sah.*

## *Tempo Mengalami DDoS*

Penulis: **Anton Lepari**

Belum lama ini, Tempo.co, salah satu portal berita terbesar di Indonesia, mengalami serangan DDoS yang menyebabkan situs mereka sulit diakses oleh pembaca selama beberapa waktu. DDoS (*Distributed Denial of Service*) adalah upaya menyerang sistem komputer, server, atau jaringan dengan cara membanjirinya dengan lalu lintas internet yang luar biasa besar dari berbagai sumber. Tujuannya adalah membuat layanan tersebut menjadi lambat, tidak stabil, atau bahkan sepenuhnya tidak dapat diakses oleh pengguna sah.

Berbeda dengan serangan biasa yang datang dari satu sumber, serangan DDoS melibatkan ribuan bahkan jutaan perangkat yang sudah dikompromikan (sering disebut botnet) untuk meluncurkan serangan secara bersamaan.
kacau.

### Tentakel Judi Kamboja

Situs berita Tempo mengalami serangan siber jenis Distributed Denial of Service (DDoS) usai menerbitkan laporan berjudul *"Tentakel Judi Kamboja"*. Wakil Pemimpin Redaksi Tempo, Bagja Hidayat, mengungkapkan bahwa serangan mulai terjadi sejak Minggu siang, 6 April 2025. “Beberapa jam setelah artikel judi *online* terbit. Sampai hari ini sudah lebih dari 700 juta *request* DDoS,” ujar Bagja pada Rabu, 9 April 2025.

Bagja menjelaskan bahwa pada awalnya, serangan berasal dari server yang terlacak di Jerman. Namun, seiring waktu, sumber serangan meluas ke berbagai negara lain, termasuk Kamboja. Ia menambahkan bahwa hingga Rabu, intensitas serangan masih terus meningkat.

### Bukan Pertama Kali

Tempo bukan kali ini saja menjadi sasaran serangan DDoS. Sebelumnya, Tempo juga mengalami serangan serupa setelah redaksi menerima ancaman berupa kiriman kepala babi pada 20 Maret 2025. Namun, menurut Bagja Hidayat, skala serangan kali ini jauh lebih besar dibandingkan insiden sebelumnya.

*Chief Technology Officer* PT Info Media Digital (penerbit Tempo.co), Heru Tjatur, menjelaskan bahwa hanya dalam rentang waktu pukul 12.45 hingga 14.48 WIB siang tadi, sistem mencatat adanya 478 juta permintaan ke server. Dari jumlah tersebut, 340 juta berhasil difilter, 95 juta diblokir, dan 26 juta koneksi diputus secara langsung.

"Kalau *firewall* kami gagal mengenali pola, potensi serangannya bisa makin besar. Akibatnya, server akan semakin berat dan bisa tumbang," ujar Tjatur.

Lebih lanjut, pada pukul 17.00 WIB, intensitas serangan tercatat melonjak hingga dua kali lipat. Secara keseluruhan, dalam tiga hari terakhir, Tempo menerima 1,7 miliar permintaan berbahaya. Investigasi menunjukkan bahwa sebagian besar lalu lintas tersebut berasal dari penyedia internet lokal seperti MSN dan Telkomnet (bagian dari Telkom Group), sehingga layanan lain yang menggunakan infrastruktur serupa turut terdampak.

### Sumber


- Tempo. (9 April 2025). *Tempo Diserang DDoS Setelah Terbitkan Liputan Judi Online*. https://www.tempo.co/hukum/tempo-diserang-ddos-setelah-terbitkan-liputan-judi-online--1229214
- Kamsib Indonesia. (2025). *Majalah Kamsib Indonesia on Paper* (Edisi 9, 31 Maret–6 April 2025). Kamsib Indonesia.
- Tempo. (12 April 2025). *Mengenal Serangan Siber DDoS ke Tempo Berkali-kali*. https://www.tempo.co/sains/mengenal-serangan-siber-ddos-ke-tempo-berkali-kali-1230346


*Penting untuk dicatat bahwa melakukan serangan DDoS, dengan atau tanpa bantuan AI, adalah ilegal dan bertentangan dengan etika professional.*

## *Melakukan DDoS dengan Bantuan AI*

Penulis: **Anton Lepari**

Melakukan serangan *Distributed Denial of Service* (DDoS) dengan bantuan kecerdasan buatan (AI) merupakan topik yang semakin mendapat perhatian dalam penelitian keamanan siber. Meskipun penggunaan AI dalam serangan DDoS masih dalam tahap eksplorasi, beberapa studi telah menyoroti potensi AI dalam meningkatkan efektivitas serangan ini.

### Pemanfaatan AI dalam Serangan DDoS

Berikut ini adalah beberapa konsep yang bisa dilakukan untuk memanfaatkan AI dalam serangan DDoS. Kita perlu mencatat bahwa melakukan serangan DDoS, dengan atau tanpa bantuan AI, adalah ilegal dan bertentangan dengan etika profesional.

1. **Pemilihan Target yang Efisien**: AI dapat digunakan untuk menganalisis jaringan dan mengidentifikasi titik-titik lemah yang paling rentan terhadap serangan DDoS.
2. **Pengoptimalan Lalu Lintas Serangan**: Dengan pembelajaran mesin, AI dapat menyesuaikan pola lalu lintas serangan agar menyerupai lalu lintas normal, sehingga lebih sulit dideteksi oleh sistem pertahanan.
3. **Adaptasi Terhadap Pertahanan**: AI memungkinkan serangan untuk beradaptasi secara *real-time* terhadap perubahan dalam sistem pertahanan target, meningkatkan kemungkinan keberhasilan serangan.
4. **Automatisasi Serangan**: AI dapat mengotomatiskan proses serangan, mengurangi kebutuhan intervensi manusia dan memungkinkan serangan yang lebih cepat dan efisien.

Teori mengenai penggunaan AI dalam serangan DDoS perlu diuji dan dibuktikan dalam praktik teknis agar dapat dipahami lebih dalam dampaknya

dan efektivitasnya. Implementasi konsep ini dalam dunia nyata juga memiliki tantangan besar, baik dari sisi teknis, etika, maupun hukum.

## Studi Ilmiah Terkait

Beberapa penelitian telah membahas penggunaan AI dalam konteks serangan DDoS:

- *"Artificial intelligence for cybersecurity: Literature review and future research directions"* oleh Ramanpreet Kaur, Dušan Gabrijelčič, dan Tomaž Klobučar (2023) membahas bagaimana AI dapat digunakan dalam berbagai aspek keamanan siber, termasuk potensi penggunaannya dalam serangan.
- *"Detecting Denial of Service attacks using machine learning algorithms*" oleh Kumari, K. dan Mrunalini, M. (2022) menyoroti bagaimana pembelajaran mesin dapat digunakan untuk mendeteksi dan memitigasi serangan DDoS.

## Etika dan Legalitas

Penting untuk dicatat bahwa melakukan serangan DDoS, dengan atau tanpa bantuan AI, adalah ilegal dan bertentangan dengan etika profesional. Tujuan dari pembahasan ini adalah untuk meningkatkan kesadaran tentang potensi ancaman dan mendorong pengembangan sistem pertahanan yang lebih baik.

## Sumber


- Ramanpreet Kaur, Dušan Gabrijelčič, Tomaž Klobučar, *Artificial intelligence for cybersecurity: Literature review and future research directions*, Information Fusion, Volume 97, 2023, 101804, ISSN 1566-2535, https://doi.org/10.1016/j.inffus.2023.101804.
- Kumari, K., Mrunalini, M. *Detecting Denial of Service attacks using machine learning algorithms*. J Big Data 9, 56 (2022). https://doi.org/10.1186/s40537-022-00616-0


*Salah satu ancaman utama yang dibawa oleh quantum computing adalah kemampuannya untuk memecahkan sistem kriptografi yang saat ini digunakan untuk melindungi data dan komunikasi di seluruh dunia.*

# *Pengenalan Quantum Computing dan Masa Depan dalam Keamanan Siber*

Penulis: **Anton Lepari**

*Quantum Computing* adalah jenis komputer yang menggunakan prinsip-prinsip fisika kuantum untuk memproses informasi. Berbeda dengan komputer biasa yang menggunakan bit (0 atau 1), komputer kuantum menggunakan *qubit*, yang bisa berada di banyak keadaan sekaligus (superposisi). Hal ini memungkinkan komputer kuantum untuk melakukan banyak perhitungan secara bersamaan, yang sangat cepat dibandingkan komputer biasa.

Bayangkan kamu punya bola mainan yang bisa berada di dua tempat sekaligus, di atas meja dan di bawah meja. Biasanya, bola hanya bisa berada di satu tempat saja, kan? Tapi dengan komputer kuantum, bola bisa ada di dua tempat bersamaan, dan itu membuatnya sangat cepat dalam melakukan banyak hal dalam waktu yang sama! Jadi, komputer kuantum bisa melakukan banyak pekerjaan lebih cepat dibandingkan komputer biasa.

Untuk memanfaatkan potensi komputasi kuantum, *qubit* harus terlebih dahulu di-*entangle* (disambungkan) untuk memanfaatkan kekuatan komputasi eksponensialnya. Setelah itu, operator melakukan operasi pada *qubit*, seperti penjumlahan, perkalian, atau perhitungan yang lebih rumit. Tergantung pada jenis komputer kuantum, sinyal elektromagnetik atau laser digunakan untuk menciptakan *entanglement* dan operasi tersebut.

Namun, meskipun memiliki potensi besar, komputer kuantum masih dalam tahap pengembangan dan menghadapi tantangan teknis yang signifikan sebelum dapat digunakan secara luas.

## Masa Depan Quantum Computing dalam Keamanan Siber

*Quantum computing* dapat mempercepat penyelesaian masalah yang sebelumnya sangat sulit atau memakan waktu lama dengan komputasi klasik. Ini memiliki potensi untuk mempercepat dan meningkatkan algoritma dalam *artificial intelligence* (AI) dan *machine learning* (ML). Hal ini akan mempengaruhi banyak aspek, seperti analisis data besar, prediksi, dan pengenalan pola.

Dalam AI, mengenali pola dalam data besar adalah kunci untuk membuat prediksi yang akurat. Dengan kemampuan *quantum computing* dalam menangani data dalam jumlah besar lebih cepat dan efisien, proses pembelajaran mesin dapat dilakukan lebih cepat. Misalnya, dalam aplikasi pengenalan gambar atau teks, quantum computing bisa mempercepat pelatihan model, memungkinkan AI untuk belajar lebih cepat dan lebih akurat.

Salah satu ancaman utama yang dibawa oleh *quantum computing* adalah kemampuannya untuk memecahkan sistem kriptografi yang saat ini digunakan untuk melindungi data dan komunikasi di seluruh dunia.

## Sumber


- NIST. *Quantum Computing Explained*. https://www.nist.gov/quantum-information-science/quantum-computing-explained
- Josh Schneider dan Ian Smalley. What is quantum computing?. IBM. https://www.ibm.com/think/topics/quantum-computing
- Niu, Chence & Irannezhad, Elnaz & Myers, Casey & Dixit, Vinayak. (2025). *Quantum Computing in Transport Science: A Review*. 10.48550/arXiv.2503.21302



**Kamsib Indonesia**
Jakarta, Indonesia
hubungi@kamsib.id



***Kamsib ID*** *adalah sebuah platform edukasi yang berfokus pada keamanan informasi dan siber dalam bahasa Indonesia. Kehadiran Kamsib dipicu oleh lonjakan pesat penggunaan internet yang tidak diimbangi dengan kesadaran akan pentingnya keamanan di dunia maya. Fenomena ini juga menjadi salah satu pemicu dari banyaknya kasus penipuan, kebocoran data, dan insiden dalam sistem elektronik, baik yang dimiliki oleh pemerintah maupun swasta.*

***Kamsib Indonesia on Paper*** *adalah majalah yang membahas berbagai aspek keamanan siber, mulai dari ancaman terbaru, teknik perlindungan, hingga tren teknologi yang memengaruhi lanskap keamanan digital. Diterbitkan secara berkala, majalah ini menyajikan artikel mendalam, studi kasus, serta wawancara dengan para ahli untuk memberikan wawasan bagi profesional keamanan siber, peneliti, dan penggemar dunia siber. Dengan pendekatan yang informatif dan analitis, Kamsib Indonesia on Paper bertujuan menjadi referensi utama bagi siapa saja yang ingin memahami dan menghadapi tantangan di dunia siber yang terus berkembang.* [at]kamsib_id